Security & Safety

IGEL Product Security Information

Here you find all IGEL Security Notices (ISNs). They inform you of any major vulnerabilities that have been found in IGEL software products and of how to fix or mitigate these. If you have questions or concerns about ISNs, you can contact the IGEL Security Team at security@igel.com[1]. If you are an IGEL customer, please open a case on the IGEL Customer Portal[2].

Besides that, most IGEL software updates fix several minor vulnerabilities. You find information about these in the Release Notes that are published with each release.

Security Announcements Mailing List
To get new ISNs and ISN updates delivered to your inbox, subscribe to the Security Announcements Mailing List. Go to igel.com[3] and find the "Subscribe for Updates" form at the bottom of the page.
This will initially subscribe you to all mailings from IGEL, but using the unsubscribe link at the bottom of a mail, you can select which communications you wish to receive and which not.

IGEL Security Notices (ISN)

1. mailto:security@igel.com
2. https://support.igel.com/
3. http://igel.com

ISN 2025-47: IGEL Citrix Workspace App Package Vulnerability

First published 3 November 2025

CVSS:3.1: 8.3 (High)

CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:L

Summary

A security vulnerability has been found in the Citrix Workspace App (CWA) package for IGEL OS. This affects the following product versions:

- IGEL OS 12

Details

A security issue has been found in the IGEL packages for Citrix Workspace App (CWA) released since 2503 Build 2 (17 June 2025): When changing the configuration from an Active Directory user to a local user on OS 12, it is still possible to log in as the Active Directory user via the cached Kerberos passthrough authentication.

Update Instructions

- OS 12: Update to the Citrix Workspace App (CWA) in version 2505 Build 2 or newer when available from the IGEL App Portal.

ISN 2025-46: Webkit Vulnerability

First published 20 October 2025

CVSS:3.1: 8.8 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

A security vulnerability has been found in Webkit, a web browser engine used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

It has been discovered that processing maliciously crafted web content with Webkit may lead to an unexpected process crash. This is known as CVE-2025-43343 and is rated as critical by CISA. IGEL downgrades the rating to high for the IGEL OS context, because there, Webkit is only used to access well-known URLs and not arbitrary web content.

Update Instructions

- OS 12: Update to the OS 12 base system app in version 12.7.4 or newer when available from the IGEL App Portal.
- OS 11: Update to IGEL OS version 11.11.100 when available.

References

- CVE-2025-43343 at NVD: https://nvd.nist.gov/vuln/detail/CVE-2025-43343

ISN 2025-45 LibTiff Vulnerability

First published 14 October 2025

CVSS:3.1: 8.8 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

A security vulnerability has been found in LibTiff, an image processing library used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

LibTiff suffers from a write-what-where condition that can be triggered by processing a specially crafted TIFF image file. This means that an attacker could write outside of bounds, execute arbitrary code, or crash the application. This is tracked as CVE-2025-9900 and rated high.

Update Instructions

- OS 12: Update to the OS 12 base system app in version 12.7.4 or newer when available from the IGEL App Portal.
- OS 11: Update to IGEL OS version 11.11.100 when available.

References

- CVE-2025-9900 at NVD: https://nvd.nist.gov/vuln/detail/CVE-2025-9900

ISN 2025-44 Chromium Vulnerabilities

First published 13 October 2025

CVSS:3.1: 8.1 (High)

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

Multiple security vulnerabilities have been found in Chromium, a web browser used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

Heap buffer overflows have been discovered in the components WebGPU (CVE-2025-11205, high), Video (CVE-2025-11206, high), and Sync (CVE-2025-11458, high). These may lead to crashes or execution of arbitrary code. Also, the V8 JavaScript engine is affected by two instances of heap buffer overflow, in WebGPU (CVE-2025-11205, high) and Video (CVE-2025-11206, high).

Apart from that, information can be leaked from V8 via a side channel (CVE-2025-10890). The Storage component contains a use-after-free, which could crash Chromium or execute arbitrary code (CVE-2025-11460, high).

Update Instructions

- OS 12: Update to the Chromium app in version 141.0.7390.65 or newer when available from the IGEL App Portal.
- OS 11: Update to IGEL OS version 11.11.100 when available.

References

- Chrome Releases Blog: https://chromereleases.googleblog.com/2025/10/stable-channel-update-for-desktop.html
- Chrome Releases Blog: https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_30.html
- Chrome Releases Blog: https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_23.html

ISN 2025-43: OpenSSL Vulnerability

First published 13 October 2025

CVSS:3.1: 7.5 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Summary

A security vulnerability has been found in OpenSSL, a cryptography library and toolkit used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

It has been discovered that decrypting Cryptographic Message Syntax (CMS) messages encrypted using password-based encryption can trigger an out-of-bounds read and write (CVE-2025-9230, high). This may crash the application using the OpenSSL library or even enable the execution of arbitrary code.

Update Instructions

- OS 12: Update to the IGEL OS base system app in version 12.7.4 or newer when available from the IGEL App Portal.
- OS 11: Update to IGEL OS version 11.11.100 when available.

References

OpenSSL Security Advisory [30th September 2025]: https://openssl-library.org/news/secadv/20250930.txt

ISN 2025-42: ImageMagick Vulnerabilities

First published 2 October 2025

CVSS:3.1: 8.8 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

Multiple security vulnerabilities have been found in ImageMagick, an open-source image processor used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

It has been discovered that a format string vulnerability exists in the InterpretImageFilename function where user input is directly passed to FormatLocaleString without proper sanitization. An attacker can use this to overwrite arbitrary memory regions, enabling a wide range of attacks from heap overflow to remote code execution (CVE-2025-55298, high).

Apart from that the magnified size calculations in ReadOneMNGIMage are unsafe and can overflow, leading to memory corruption (CVE-2025-55154, high). Finally, a possible division by zero via the montage command can crash the program (CVE-2025-55212, high).

Update Instructions

- OS 12: Update to the IGEL OS base system app in version 12.7.4 or newer when available from the IGEL App Portal.
- OS 11: Update to IGEL OS version 11.11.100 when available.

References

Debian Security Advisory DSA-5997-1: https://lists.debian.org/debian-security-announce/2025/msg00161.html

ISN 2025-41: CUPS Vulnerability

First published 1 October 2025

CVSS:3.1: 8.8 (High)

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

Summary

A security vulnerability has been found in CUPS, an open-source printing system used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

It has been found that CUPS suffers from an authentication bypass: If the AuthType is set to anything but Basic, and the request contains an `Authorization: Basic ...` header, the password is not checked. This is tracked as CVE-2025-58060 and rated as high.

Update Instructions

- OS 12: Update to the IGEL OS base system app in version 12.7.3 or newer when available from the IGEL App Portal.
- OS 11: Update to IGEL OS version 11.11.100 when available.

References

- CVE-2025-58060: https://nvd.nist.gov/vuln/detail/CVE-2025-58060

ISN 2025-39: Webkit Vulnerability

First published 2 October 2025

CVSS:3.1: 8.8 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

A security vulnerability has been found in Webkit, a web browser engine used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

It has been discovered that processing maliciously crafted web content with Webkit may lead to an unexpected process crash. This is known as CVE-2025-43342 and rated as critical by CISA. IGEL downgrades the rating to high for the IGEL OS context, because there Webkit is only used to access well-known URLs and not arbitrary web content.

Update Instructions

- OS 12: Update to the OS 12 base system in version 12.7.3 or newer when available from the IGEL App Portal.
- OS 11: Update to IGEL OS version 11.11.100 when available.

References

- WebKitGTK and WPE WebKit Security Advisory WSA-2025-0006: https://webkitgtk.org/security/WSA-2025-0006.html

ISN 2025-38: Critical Chromium Vulnerabilities CVE-2025-10200 & CVE-2025-10585

First published 21 October 2025

- CVSS:3.1: 9.8- Critical (CVE-2025-10200)
- Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

- CVSS:3.1: 9.8- Critical (CVE-2025-10585)
- Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

- CVSS: 3.1: 8.8-High (CVE-2025-10201)
- Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

- CVSS 3.1 : 8.8-High (CVE-2025-10500)
- Vector String : CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

- CVSS 3.1: 8.8-High (CVE-2025-10501)
- Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

- CVSS 3.1: 8.8-High (CVE-2025-10502)
- Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

A number of security vulnerabilities have been found in Chromium, a web browser used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

One is tracked as CVE-2025-10200 and rated high by NVD.
IGEL does not consider any user interaction as necessary, which changes the rating to “critical” according to the Vector String specified above.

Critical CVE-2025-10200[4]: Use after free in Serviceworker in Google Chrome on Desktop prior to 140.0.7339.127 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical) [NIST]

4. https://nvd.nist.gov/vuln/detail/CVE-2025-10200

Critical CVE-2025-10585[5]: Type confusion in V8 in Google Chrome prior to 140.0.7339.185 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. This CVE is documented to be exploited in the wild by CISA(BOD 22-01)[6] and is included in the Known Exploited Vulnerabilities Catalog[7] since 23rd of September. For further information please visit the linked Webpages.

High CVE-2025-10201[8]: Inappropriate implementation in Mojo in Google Chrome on Android, Linux, ChromeOS prior to 140.0.7339.127 allowed a remote attacker to bypass site isolation via a crafted HTML page. (Chromium security severity: High) [NIST]

High CVE-2025-10500[9]: Use after free in Dawn in Google Chrome prior to 140.0.7339.185 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)

High CVE-2025-10501:[10] Use after free in WebRTC in Google Chrome prior to 140.0.7339.185 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)

High CVE-2025-10502[11]: Heap buffer overflow in ANGLE in Google Chrome prior to 140.0.7339.185 allowed a remote attacker to potentially exploit heap corruption via malicious network traffic. (Chromium security severity: High)

Update Instructions

- OS 12: Update to the Chromium app in version 140.0.7339.185 or newer from the IGEL App Portal.
- OS 11: Update to IGEL OS version 11.10.430 or newer.

References

- Chrome Releases Blog(9th September): https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_9.html https://chromium.googlesource.com/chromium/src/+log/140.0.7339.81..140.0.7339.133?pretty=fuller&n=10000
- Chrome Releases Blog (17th September): https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_17.html

5. https://nvd.nist.gov/vuln/detail/CVE-2025-10585
6. https://www.cisa.gov/news-events/directives/bod-22-01-reducing-significant-risk-known-exploited-vulnerabilities
7. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
8. https://nvd.nist.gov/vuln/detail/CVE-2025-10201
9. https://nvd.nist.gov/vuln/detail/CVE-2025-10500
10. https://nvd.nist.gov/vuln/detail/CVE-2025-10501
11. https://nvd.nist.gov/vuln/detail/CVE-2025-10502

ISN 2025-37: Critical Chromium Vulnerability

First published 2 September 2025

CVSS:3.1: N/A - Critical

CVSS:3.1/N/A

Summary

A security vulnerability has been found in Chromium, a web browser used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

A use-after-free vulnerability has been found in the ANGLE (Almost Native Graphics Layer Engine) component. This can crash the application or enable the execution of arbitrary code. It is tracked as CVE-2025-9478 and rated critical.

Update Instructions

- OS 12: Update to the Chromium app in version 139.0.7258.154 or newer when available from the IGEL App Portal.
- OS 11: Update to IGEL OS version 11.10.420 when available.

References

- Chrome Releases Blog: https://chromereleases.googleblog.com/2025/08/stable-channel-update-for-desktop_26.html

ISN 2025-36: Firefox ESR Vulnerabilities

Updated 1 October (fix version)

First published 2 September

CVSS:3.1: 8.3 (High)

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

Multiple security vulnerabilities have been found in Firefox ESR, a web browser used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

It has been discovered that an attacker could perform memory corruption in the GMP process, which processes encrypted media. This is rated as high and tracked as CVE-2025-9179. The Graphics: Canvas2D component is affected by a bypass in the Same-origin Policy (CVE-2025-9180, high). Apart from that, several memory safety bugs have been found that could enable arbitrary code execution or crash the application (CVE-2025-9185, high).

Update Instructions

- OS 12: Update to the Firefox ESR app in version 128.14 or newer from the IGEL App Portal.
- OS 11: Update to IGEL OS version 11.10.430.

References

- Mozilla Foundation Security Advisory 2025-66: https://www.mozilla.org/en-US/security/advisories/mfsa2025-66/

ISN 2025-35: JRE Vulnerabilities

First published 21 August 2025

CVSS:3.1: 8.1 (High)

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

Multiple security vulnerabilities have been found in Azul Zulu, a JRE distribution used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

Three findings rated high affect installations that run Java Web Start applications or sandboxed Java applets and that rely on the Java sandbox for security. These difficult-to-exploit vulnerabilities allow an unauthenticated attacker with network access to compromise the Java VM (CVE-2025-30749, CVE-2025-50106, CVE-2025-50059).

Apart from this, the packaged Libxslt suffers from a use-after-free vulnerability (CVE-2025-24855, high). This may lead to a crash or execution of arbitrary code.

Update Instructions

- OS 12: Update to the Java Runtime Environment OS 12 app in version 17.0.16 or newer.
- OS 11: Update to IGEL OS version 11.11.100 when available.

References

- CVE-2025-30749 https://www.cve.org/CVERecord?id=CVE-2025-30749
- CVE-2025-50059: https://www.cve.org/CVERecord?id=CVE-2025-50059
- CVE-2025-50106: https://www.cve.org/CVERecord?id=CVE-2025-50106
- CVE-2025-24855 https://www.cve.org/CVERecord?id=CVE-2025-24855

ISN 2025-34: Libarchive Vulnerability

First published 14 August 2025

CVSS:3.1: 7.8 (High)

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

Summary

A security vulnerability has been found in Libarchive, a compression library used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

A memory management issue has been discovered in the Libarchive library, specifically within the “archive_read_format_rar_seek_data()” function. It involves an integer overflow that can ultimately lead to a double free, causing a crash or enabling code execution (CVE-2025-5914).

This vulnerability has recently been ranked up to critical by NVD. However, as it only occurs on systems with large memory (> 100 GB), which is untypical for IGEL OS, IGEL is rating it down to high.

Update Instructions

- OS 12: Update to the IGEL OS base system app in version 12.7.1 PR1 or newer when available from the IGEL App Portal.
- OS 11: Update to IGEL OS version 11.11.100 when available.

References

- CVE-2025-5914 at NVD: https://nvd.nist.gov/vuln/detail/CVE-2025-5914
- Libarchive Pull Request - Fix double free with over 4 billion nodes: https://github.com/libarchive/libarchive/pull/2598

ISN 2025-33: Chromium Vulnerabilities

First published 12 August 2025

CVSS:3.1: 8.8 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

Multiple security vulnerabilities have been found in Chromium, a web browser used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

Two instances of type confusion in Chromium's JavaScript engine V8 may allow a remote attacker to exploit heap corruption via a crafted HTML page (CVE-2025-8010 and CVE-2025-8011, both rated high). Besides this, the Media Stream component has been found to contain a use-after-free (CVE-2025-8292, high).

Update Instructions

- OS 12: Update to IGEL OS 12 Chromium app version 139.0.7258.66 or newer when available from the IGEL App Portal.
- OS 11: Update to IGEL OS version 11.11.100 when available.

References

- Chrome Releases Blog: https://chromereleases.googleblog.com/2025/08/stable-channel-update-for-desktop.html
- Chrome Releases Blog: https://chromereleases.googleblog.com/2025/07/stable-channel-update-for-desktop_29.html

ISN 2025-32: Webkit Vulnerabilities

First published 12 August 2025

CVSS:3.1: 8.8 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

Multiple security vulnerabilities have been found in Webkit, a web browser engine used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

Webkit contains three vulnerabilities that may lead to memory corruption when processing maliciously crafted web content (CVE-2025-24189, CVE-2025-31273, CVE-2025-31278, all high). CVE-2025-43227, rated high, may disclose sensitive user information. Finally, malicious web content can lead to an application crash (CVE-2025-6558, high).

Google is aware that an exploit for CVE-2025-6558 exists in the wild.

Update Instructions

- OS 12: Update to IGEL OS 12 Base system app version 12.8.1 when available from the IGEL App Portal.
- OS 11: Update to IGEL OS version 11.11.100 when available.

References

- WebKitGTK and WPE WebKit Security Advisory WSA-2025-0005: https://webkitgtk.org/security/WSA-2025-0005.html

ISN 2025-31: XSS Vulnerabilities in UMS

First published 28 July 2025

CVSS:3.1: 8.0 (High)

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

Summary

Multiple instances of Stored Cross-Site Scripting (XSS) vulnerabilities found that affect the following products:

- IGEL Universal Management Suite versions <=12.08.110

Details

After internal and external security testing, multiple instances of stored Cross-Site Scripting (XSS) vulnerabilities have been found in IGEL UMS. The vulnerability potentially allow a low privilege UMS admin to escalate its privileges through cookie/session hijacking.

Update Instructions

- UMS: Update to version 12.08.130

ISN 2025-30: Firefox ESR Vulnerabilities

First published 4 August 2025

CVSS:3.1: 8.8 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

Security vulnerabilities have been found in Firefox ESR, a web browser used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

The JavaScript compiler Monkey-JIT writes only 32 bits of the 64-bit return value space on the stack, while the component Baseline-JIT reads the entire 64 bits (CVE-2025-8027, high). Besides that, the Mozilla Fuzzing Team have discovered multiple memory safety bugs that might be exploited to execute arbitrary code (CVE-2025-8034 and CVE-2025-8035, high).

Update Instructions

- OS 12: Update to the Firefox ESR app in version 128.13 or newer when available from the IGEL App Portal.
- OS 11: Update to IGEL OS version 11.11.100 when available.

References

- Mozilla Foundation Security Advisory 2025-62: https://www.mozilla.org/en-US/security/advisories/mfsa2025-62/
- Mozilla Foundation Security Advisory 2025-57: https://www.mozilla.org/en-US/security/advisories/mfsa2025-57/

ISN 2025-29: Chromium Vulnerability in ANGLE Exploited in the Wild

First published 4 August 2025

CVSS:3.1: 8.8 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

A security vulnerability has been found in Chromium, a web browser used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

It has been discovered that Chromium's Almost Native Graphics Layer Engine (ANGLE) and its GPU compositor do not correctly validate untrusted input. This is tracked as CVE-2025-6558 and rated as high. Google is aware that an exploit for CVE-2025-6558 exists in the wild.

Further highs concern an integer overflow in the V8 JavaScript engine (CVE-2025-7656) and a use-after-free in WebRTC (CVE-2025-7657).

Update Instructions

- OS 12: Update to the Chromium App in version 138.0.7204.157 or newer when available from the IGEL App Portal.
- OS 11: Update to IGEL OS version 11.11.100 when available.

References

- Chrome Releases Blog: https://chromereleases.googleblog.com/2025/07/stable-channel-update-for-desktop_15.html

ISN 2025-26: Chromium Vulnerability Exploited in the Wild

Updated 9 July 2025 (Corrected Chromium fix version, OS 11 fix version)

First published 2 July 2025

CVSS:3.1: 8.8 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

A security vulnerability has been found in Chromium, a web browser used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

A type confusion has been found in V8, the JavaScript engine in Chromium. It can allow a remote attacker to perform arbitrary reads or writes via a crafted HTML page (CVE-2025-6554, high).
Google reports that an exploit for this vulnerability exists in the wild.

Update Instructions

- OS 12: Update to the Chromium App in version 138.0.7204.92 or newer when available from the IGEL App Portal.
- OS 11: Update to IGEL OS version 11.110.410 when available (planned for July).

References

- Chrome Releases Blog: https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop_30.html

ISN 2025-25: Firefox ESR Vulnerability

First published 2 July 2025

CVSS:3.1: 8.8 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

A security vulnerability has been found in Firefox ESR, a web browser used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

A use-after-free issue has been discovered in FontFaceSet, an interface for loading fonts. This can lead to a crash of the application, which an attacker could potentially exploit (CVE-2025-6424, high).

Update Instructions

- OS 12: Update to the Firefox ESR App in version 128.12 or newer when available from the IGEL App Portal.
- OS 11: Update to IGEL OS version 11.11.100 when available (planned for August).

References

- MFSA-2025-53: https://www.mozilla.org/en-US/security/advisories/mfsa2025-53/

ISN 2025-24: Command Execution in IGEL OS

First published 30 June 2025

CVSS:3.1: 8.8 (High)

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Summary

A security vulnerability has been found in the IGEL OS base system. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

An issue has been found in the way IGEL OS handles the LD_PRELOAD environment variable. This may enable a local user to execute arbitrary commands, even in the session of another user.

Update Instructions

- OS 12: Update to IGEL OS 12.7.1.
- OS 11: Update to IGEL OS 11.10.410 when available (planned for July).

ISN 2025-23: Chromium Vulnerability Exploited in the Wild

First published 30 June 2025

CVSS:3.1: 8.8 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

Security vulnerabilities have been found in Chromium, a web browser used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

An out-of-bounds read has been found in V8, the JavaScript engine in Chromium. It could allow a remote attacker to potentially exploit heap corruption via a crafted HTML page. This is rated as high and tracked as CVE-2025-5419.

Google reports that this issue is being exploited in the wild.

Other issues are a use-after-free in the Media component (CVE-2025-5958, high) and a type confusion in V8 (CVE-2025-5959, high).

Update Instructions

- OS 12: Update to the Chromium App in version 137.0.7151.103 or newer when available from the IGEL App Portal.
- OS 11: Update to IGEL OS version 11.10.410 when available (planned for July).

References

- Chrome Releases Blog: https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop.html
- Chrome Released Blog: https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop_10.html

ISN 2025-22: Statement on CVE-2025-47827 in IGEL OS 10

First published 2 June 2025

Summary

The researcher Zack Didcott has found an issue in IGEL OS version 10, which is no longer maintained. The current versions OS 11 and OS 12 are not affected.

Details

Generally, IGEL only issues IGEL Security Notices (ISN) for product versions that are in active maintenance. However, this ISN is about IGEL OS 10, a version that is no longer maintained with security fixes and should not be used in productive environments. IGEL publishes this as a reaction to the publication of CVE-2025-47827, only for clarification and for the sake of completeness.

Zack Didcott describes an issue in the integrity of the boot chain in OS 10. It uses UEFI Secure Boot, but the Linux kernel does not verify the cryptographic signature of the system partition. This can enable an attacker to boot a different system partition.

IGEL wants to emphasize that while Secure Boot is a part of the core security principles in IGEL OS, booted kernels, and hence system images, need to undergo frequent patching of vulnerabilities. Unmaintained kernels and systems such as OS 10 pose a general security risk to the user, not only in terms of the Secure Boot chain.

For clarity: This does not affect IGEL OS 11 and OS 12, who do check the signatures of all partitions.

Update Instructions

Update systems to actively maintained products.

There is no need for any action for users of the current versions IGEL OS 11 and OS 12.

References

- CVE-2025-47827
- https://github.com/Zedeldi/CVE-2025-47827

ISN 2025-21: Glibc Vulnerability

First published 3 June 2025

CVSS 3.1: 7.8 (High)

CVSS 3.1: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

A security vulnerability has been discovered in Glibc, the C library used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

The GNU C library (Glib) has a vulnerability in handling the LD_LIBRARY_PATH environment variable in statically linked SetUID binaries that call dlopen. The issue may cause library code to be loaded that is under control of an attacker.

This vulnerability was initially rated as critical but was later downgraded to high, as it became clear that it can only be exploited locally, not from the network.

Update Instructions

- OS 12: Update to OS 12.7.0 when available (planned for 4 June).
- OS 11: Update to 11.10.310 when available (planned for 4 June).

References

- CVE-2025-4802: https://www.cve.org/CVERecord?id=CVE-2025-4802

ISN 2025-20: Critical Firefox ESR Vulnerabilities

First published 3 June 2025

CVSS 3.1: 9.8 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

Security vulnerabilities have been discovered in Firefox ESR, a web browser used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

Three critical issues affect Firefox ESR: CVE-2025-4918 is an out-of-bounds read or write on a JavaScript Promise object. CVE-2025-4919 can enable an out-of-bounds read or write on a JavaScript object by confusing array index sizes. Finally, a double-free can occur in the libvpx encoder used for WebRTC (MFSA-TMP-2025-0001). These vulnerabilities can allow a remote attacker to crash the application, execute code or read data.

Update Instructions

- OS 12: Update to the OS 12 Firefox ESR app version 128.11 or newer when available from the IGEL App Portal.
- OS 11: Update to 11.10.310 when available (planned for 4 June).

References

- Mozilla Foundation Security Advisory 2025-44: https://www.mozilla.org/en-US/security/advisories/mfsa2025-44/
- Mozilla Foundation Security Advisory 2025-37: https://www.mozilla.org/en-US/security/advisories/mfsa2025-37/

ISN 2025-19: Chromium Vulnerability Exploited in the Wild

First published 3 June 2025

CVSS 3.1: 8.8 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

Security vulnerabilities have been discovered in Chromium, a web browser used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

Chromium is affected by two security issues that Google rates as high: CVE-2025-4664 concerns insufficient policy enforcement in the Loader component. CVE-2025-4609 is an incorrect handle provided in unspecified circumstances in the Mojo component.

Google is aware of reports that an exploit for CVE-2025-4664 exists in the wild and has not disclosed more details about the vulnerabilities so far.

Update Instructions

- OS 12: Update to the OS 12 Chromium app in version 136.0.7103.113 or newer when available from the IGEL App Portal.
- OS 11: Update to 11.10.310 when available (planned for 4 June).

References

- Chrome Releases Blog: https://chromereleases.googleblog.com/2025/05/stable-channel-update-for-desktop_14.html

ISN 2025-18: Critical Libsoup Vulnerability

First published 26 May 2025

CVSS 3.1: 9.0 (Critical)

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

Summary

Security vulnerabilities have been discovered in libsoup, an HTTP client/server library used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

Several security issues have been found in libsoup. CVE-2025-32911 is rated critical and concerns a use-after-free vulnerability in the treatment of HTTP headers that a remote attacker could use to cause memory corruption in the HTTP server.

Issues CVE-2025-32906 and CVE-2025-32914 are rated high and describe out-of-bounds reads that could crash the HTTP server. A libsoup client or server could also be crashed by a NULL pointer dereference (CVE-2025-32913, high).

Update Instructions

- OS 12: Update to OS 12.7.0 when available (planned for 4 June).
- OS 11: Update to OS 11.10.310 when available (planned for 4 June).

References

- CVE-2025-32911: https://www.cve.org/CVERecord?id=CVE-2025-32911
- CVE-2025-32906: https://www.cve.org/CVERecord?id=CVE-2025-32906
- CVE-2025-32914: https://www.cve.org/CVERecord?id=CVE-2025-32914
- CVE-2025-32913: https://www.cve.org/CVERecord?id=CVE-2025-32913

ISN 2025-17: Vulnerabilities in NVIDIA Graphics Driver

Updated 6 October 2025 (further CVEs, OS 12 fix version)

First published 24 June 2025

CVSS 3.1: 7.8 (High)

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Summary

Security vulnerabilities have been discovered in the NVDIA GPU driver, used in IGEL OS for NVIDIA graphics hardware. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

It has been found that the NVDIA GPU driver before version 535.247.01 has an authorization issue that could allow an unprivileged attacker to escalate privilege. A successful exploit of this vulnerability might lead to code execution, denial of service, information disclosure, and data tampering. (CVE-2025-23244, high)

Apart from this, NVIDIA lists a vulnerability where an attacker could read invalid memory. A successful exploit of this vulnerability might lead to information disclosure (CVE-2025-23286, high). CVE-2025-23279 concerns the installer only, so it does not affect IGEL OS, which does not contain the installer.

Update Instructions

- OS 12: Update to OS 12.7.4 when available (planned for December).
- OS 11: Update to OS 11.11.100 when available (planned end of November).

References

- CVE-2025-23244: https://www.cve.org/CVERecord?id=CVE-2025-23244
- Security Bulletin: NVIDIA GPU Display Driver - July 2025: https://nvidia.custhelp.com/app/answers/detail/a_id/5670
- Security Bulletin: NVIDIA GPU Display Driver - April 2025: https://nvidia.custhelp.com/app/answers/detail/a_id/5630

[CORRECTED] ISN 2025-16: Critical Vulnerability in Ppp

Corrected 25 June 2025 (not affected)

First published 23 June 2025

Summary

IGEL OS 12 and OS 11 are not affected by CVE-2024-58250.

References

- CVE-2024-58250: https://www.cve.org/CVERecord?id=CVE-2024-58250
- Jeffrey Bencteux on CVE-2024-58250: https://www.bencteux.fr/posts/cve_pppd/

ISN 2025-15: Perl Vulnerability

Updated 6 October 2025 (updated fix versions)

First published 23 June 2025

CVSS 3.1: 8.6 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

Summary

A security vulnerability has been found in Perl, a scripting language used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

A heap buffer overflow vulnerability was discovered in how Perl handles non-ASCII bytes in the left-hand-side of the ‘tr’ operator. This can crash the process and potentially enable code execution. It is tracked as CVE-2024-56406 and rated as high.

Update Instructions

- OS 12: Update to IGEL OS 12.7.2.
- OS 11: Update to IGEL OS 11.11.100 when available (planned for end of November).

References

- CVE-2024-56406: https://www.cve.org/CVERecord?id=CVE-2024-56406

ISN 2025-14: Critical IGEL OS Privilege Escalation

Updated 6 May 2025 (corrected an error in fix versions)

First published 5 May 2025

Critical

CVSS:3.1 n/a

Summary

A security vulnerability has been found in the IGEL OS network configuration mechanism. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

A vulnerability of the privilege escalation type has been found in the IGEL OS network configuration mechanism. It could enable a non-privileged user to execute commands as root. This issue is rated as critical.

Update Instructions

- OS 12: Update to IGEL OS 12.7.0 when available.
- OS 11: Update to IGEL OS 11.10.290.

ISN 2025-13: Chromium Critical Vulnerability

Updated 22 April 2025 (Fix available in OS 11.10.290)

First published 17 April 2025

CVSS 3.1: 9.0 (Critical)

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

Summary

Security vulnerabilities have been found in Chromium, a web browser used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

One of the security issues found in Chromium is a heap buffer overflow in the Codec component. Attackers could use fabricated media files to exploit this vulnerability and potentially execute code. This is tracked as CVE-2025-3619 and rated critical. The other vulnerability is a use-after-free in the USB component (CVE-2025-3620, high).

Update Instructions

- OS 12: Update the OS 12 Chromium App to version 135.0.7049.95 or newer when available.
- OS 11: Update to OS 11.10.290 when available.

References

- Chrome Release Blog: https://chromereleases.googleblog.com/2025/04/stable-channel-update-for-desktop_15.html

ISN 2025-12: Chromium Critical Vulnerability

First published 25 March 2025

CVSS 3.1: 9.6 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Summary

A security vulnerability has been found in the Chromium web browser used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

Chromium is affected by a use-after-free issue in the Lens component. A remote attacker could potentially exploit heap corruption via a crafted HTML page. This is rated as critical and tracked as CVE-2025-2476.

Mitigation

Deactivate Lens in a custom Chromium policy:

1. In Setup, go to **Chromium Browser > Global Settings > Custom Setup**.
2. Add a policy named `LensOverlaySettings` and set it to `1` (which means deactivated).

For more information, see Configuring Custom Settings[12] and (11.10.250-en) Chromium Policies for Chromium Browser Global in IGEL OS .

Update Instructions

- OS 12: Update the OS 12 Chromium App to version 134.0.6998.117 or newer when available.
- OS 11: Update to OS 11.10.270 when available (April 3rd)

References

- Chrome Release Blog: https://chromereleases.googleblog.com/2025/03/stable-channel-update-for-desktop_19.html

12. https://kb.igel.com/en/igel-apps/current/configuration-of-the-chromium-browser-in-igel-os#ConfigurationoftheChromiumBrowserinIGELOS-ConfiguringCustomSettings

ISN 2025-10: Linux Kernel Vulnerability

First published 30 April 2025

CVSS 3.1: 7.8 (High)

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Summary

A security vulnerability has been found in the Linux Kernel used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

The Linux Kernel contains an uninitialized resource vulnerability that allows an attacker to leak kernel memory via a specially crafted Human Interface Device (HID) report. Originally rated medium, IGEL rates this issue as high because CISA reports it as being used in the wild to attack Linux systems (CVE-2024-50302).

Update Instructions

- OS 12: Update to the IGEL OS base system 12.7.0 when available.
- OS 11: Update to OS 11.11.100 when available (planned for August).

References

- CVE-2024-50302 at NVD: https://nvd.nist.gov/vuln/detail/CVE-2024-50302
- CISA KEV Entry: https://www.cisa.gov/news-events/alerts/2025/03/04/cisa-adds-four-known-exploited-vulnerabilities-catalog

ISN 2025-09: Firefox ESR Vulnerabilities

First published 29 April 2025

CVSS 3.1: 8.8 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

Security vulnerabilities have been found in Mozilla Firefox ESR, a web browser used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

Mozilla reports several highs for Firefox ESR: Use-after-free issues affect the components WebTransportChild (CVE-2025-1931), XSLT (CVE-2025-1009), and Custom Highlight (CVE-2025-1010). WASM i32 return values may be corrupted in JIT on 64-bit CPUs (CVE-2025-1933).

An integer overflow when growing an SkRegion's RunArray (CVE-2024-43097) is rated as critical by Mozilla but re-ranked by IGEL as high.

Apart from that, Mozilla fixed various memory safety bugs (CVE-2025-1016 and CVE-2025-1937).

Update Instructions

- OS 12: Update to the Firefox ESR App version 115.22 from the IGEL App Portal.
- OS 11: Update OS 11.11.100 when available (planned for August).

References

- MFSA 2025-15: https://www.mozilla.org/en-US/security/advisories/mfsa2025-15/
- MFSA 2025-08: https://www.mozilla.org/en-US/security/advisories/mfsa2025-08/

ISN 2025-08: Libxml2 Vulnerabilities

First published 29 April 2025

CVSS 3.1: 7.9 (High)

CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N

Summary

Security vulnerabilities have been found in Libxml2, an XML library used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

Libxml2 is affected by a use-after-free issue that can be triggered by a crafted XML document (CVE-2024-56171). Besides that, a stack-based buffer overflow can occur during DTD validation with an untrusted DTD or document (CVE-2025-24928, high).

Update Instructions

- OS 12: Update to the IGEL OS base system 12.8.1 when available.
- OS 11: Update to OS 11.11.100 when available (planned for August).

References

- CVE-2024-56171: https://www.cve.org/CVERecord?id=CVE-2024-56171
- CVE-2025-24928: https://www.cve.org/CVERecord?id=CVE-2025-24928

ISN 2025-07: X.org Vulnerabilities

First published 27 March 2025

CVSS 3.1: 8.8 (High)

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Summary

Several security vulnerabilities have been found in X.org, the display system used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

Three of the vulnerabilities found in X.org are of the use-after-free type, which may cause the X-Server to crash or may enable an attacker to execute code: CVE-2025-26594 (high), CVE-2025-26600 (high), and CVE-2025-26601 (high). Buffer overflows have been discovered in XkbVModMaskText() (CVE-2025-26595, high) and XkbChangeTypesOfKey() (CVE-2025-26597, high), while a heap overflow affects XkbWriteKeySyms() (CVE-2025-26596, high).

Additionally, an uninitialized pointer affects the compositor (CVE-2025-26599, high), and out-of-bounds write has been found in CreatePointerBarrierClient() (CVE-2025-26598, high).

Update Instructions

- OS 12: Update to the IGEL OS base system 12.7.0 when available.
- OS 11: Update to IGEL OS 11.11.100 when available (planned for August).

References

X.Org Security Advisory: https://lists.x.org/archives/xorg-announce/2025-February/003584.html

ISN 2025-06: Critical Webkit Vulnerability

First published 21 February 2025

CVSS 3.1: 9.8 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

A security vulnerability has been found in the WebkitGTK library used in IGEL OS to render web content and UI elements. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

It has been discovered that maliciously crafted web content can crash WebkitGTK processes. This is tracked as CVE-2025-24162 and rated as critical. In addition, processing a file may lead to unexpected app termination or arbitrary code execution (CVE-2024-27856, high), and processing malicious web content can lead to memory corruption (CVE-2024-54543, high). Besides that, a privacy issue allowed remote attackers to fingerprint the user (CVE-2025-24150, high).

Update Instructions

- OS 12: Update to the IGEL OS base system 12.6.0 PR2 patch release when available.
- OS 11: Update to IGEL OS 11.10.250 when available.

References

- WSA-2025-0001: https://webkitgtk.org/security/WSA-2025-0001.html
- CVE-2025-24162 at NVD: https://nvd.nist.gov/vuln/detail/CVE-2025-24162

ISN 2025-05: HP Anyware Vulnerability

First published 5 May 2025

CVSS 3.1: 8.5 (High)

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N

Summary

A security vulnerability has been found in the HP Anyware Agent for Linux available for IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

It has been discovered that HP Anyware Agent for Linux might allow for an authentication bypass that may result in escalation of privilege. This is tracked as CVE-2025-1003 and rated as high.

Update Instructions

- OS 12: Update to the HP Anyware Agent for Linux OS 12 App in version 25.03.1 or newer from the IGEL App Portal when available.
- OS 11: Update to IGEL OS 11.11.100 when available (planned for August).

References

- HP Advisory: https://support.hp.com/us-en/document/ish_11920613-11920636-16
- CVE-2025-1003 at NVD: https://nvd.nist.gov/vuln/detail/CVE-2025-1003

ISN 2025-04: Microsoft Edge Vulnerabilities

First published 4 February 2025

CVSS 3.1: 7.4 (High)

CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Summary

Security vulnerabilities have been found in the Chromium-based Microsoft Edge web browser available as an App for IGEL OS. This affects the following product versions:

- IGEL OS 12

Details

It has been discovered that Microsoft Edge contains two escalation of privilege vulnerabilities, CVE-2025-21185 (high) and CVE-2025-21399 (high).

Besides Edge-specific issues, Edge contains issues inherited from its Chromium base. These have been closed by importing the latest fixes from Chromium.

Update Instructions

- OS 12: Update to the Microsoft Edge OS 12 app version 132.0.2957.115 or newer from the IGEL App Portal.

References

- Release notes for Microsoft Edge Security Updates: https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security

ISN 2025-03: Gstreamer Vulnerabilities

First published 15 January 2025

CVSS 3.1: 8.4 (High)

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

Several security vulnerabilities have been found in the Gstreamer multimedia framework used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

An out-of-bounds write has been discovered in the GStreamer MP4/MOV demuxer: CEA608 Closed Caption tracks can lead to crashes for certain input files (CVE-2024-47539). Another out-of-bounds write is caused by an integer overflow and tracked as CVE-2024-47537. A third vulnerability is the out-of-bounds write in the MP4/MOV demuxer and memory allocator (CVE-2024-47606). These issues would allow an attacker to crash the application and execute code by heap manipulation. IGEL rates them as high in the context of IGEL OS.

Finally, a null pointer dereference vulnerability has been found (CVE-2024-47613, high). This issue can cause a Denial of Service (DoS) by triggering a segmentation fault.

Mitigation

Until the fixed version is installed, this issue can be mitigated by not allowing users to play local MP4 files or by disabling Citrix Multimedia Redirection if multiple unexpected crashes are detected, which can be an indicator for an attack.

Update Instructions

- OS 12: Update to the OS 12.6.1 (planned for 18 February 2025).
- OS 11: Update to OS 11.10.250 (planned for 25 February 2025).

References

- GStreamer Security Advisory: https://gstreamer.freedesktop.org/security/sa-2024-0007.html
- NVD: https://nvd.nist.gov/vuln/detail/CVE-2024-47539
- NVD: https://nvd.nist.gov/vuln/detail/CVE-2024-47537
- NVD: https://nvd.nist.gov/vuln/detail/CVE-2024-47606
- NVD: https://nvd.nist.gov/vuln/detail/CVE-2024-47613

ISN 2025-02: Chromium Vulnerabilities

First published 21 January 2025

CVSS 3.1: 8.3 (High)

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Summary

Several security vulnerabilities have been identified in the Chromium web browser used in IGEL OS. This affects the following product versions:

- IGEL OS 12
- IGEL OS 11

Details

V8, Chromium's JavaScript engine is affected by two type confusions, CVE-2025-0291 (high) and CVE-2024-12692 (high). In addition, an out-of-bounds memory access has been found in V8 (CVE-2024-12693, high) as well as an out-of-bounds write (CVE-2024-12695, high).

Finally, a use-after-free has been discovered in the Compositing component (CVE-2024-12694, high).

Update Instructions

- OS 12: Update to the OS 12 Chromium App in version 132.0.6834.83 as soon as it is available on the IGEL App Portal.
- OS 11: Update to IGEL OS version 11.10.250 (planned for 25 February 2025).

References

- Chrome Releases Blog: https://chromereleases.googleblog.com/2025/01/stable-channel-update-for-desktop.html
- Chrome Releases Blog: https://chromereleases.googleblog.com/2024/12/stable-channel-update-for-desktop_18.html

ISN 2025-01: Firefox ESR Vulnerabilities

First published 21 January 2025

CVSS 3.1: 7.3 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Summary

Security vulnerabilities have been found in the Firefox ESR web browser used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

Memory safety bugs have been found in Firefox ESR. Some of these issues showed evidence of memory corruption and the Mozilla team presumes that some could have been exploited to run arbitrary code (CVE-2025-0242, high).

Update Instructions

- OS 12: Update to version 115.19 of the OS 12 Firefox app as soon as it is available on the IGEL App Portal.
- OS 11: Update to IGEL OS version 11.10.250 (planned for 25 February 2025).

References

- MSFA-2025-03: https://www.mozilla.org/en-US/security/advisories/mfsa2025-03/
- MSFA-2024-65: https://www.mozilla.org/en-US/security/advisories/mfsa2024-65/

ISN 2024-24: Chromium Vulnerability

First published 13 January 2025

CVSS 3.1: 8.8 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

A security issue has been found in the Chromium web browser used in IGEL OS. This affects the following IGEL product versions:

- IGEL OS 12
- IGEL OS 11

Details

A type confusion has been discovered in V8, Chromium's JavaScript engine. It could allow a remote attacker to exploit heap corruption via a crafted HTML page. This is tracked as CVE-2024-11395 and rated as high.

Update Instructions

- OS 12: Update to the OS 12 Chromium App version 131.0.6778.85 or newer, available from the IGEL App Portal.
- OS 11: Update to IGEL OS 11.10.250 when available.

References

- Chrome Releases Blog https://chromereleases.googleblog.com/2024/11/stable-channel-update-for-desktop_19.html
- CVE-2024-11395 Detail at NVD: https://nvd.nist.gov/vuln/detail/CVE-2024-11395

ISN 2024-23: Webkit2GTK Critical Vulnerability

Updated 13 January 2025 (OS 11 fix version)

First published 5 December 2024

CVSS 3.1: 9.2 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

A security vulnerability has been found in Webkit2GTK, a web content rendering library used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

It has been discovered that processing maliciously crafted web content in Webkit2GTK may lead to arbitrary code execution (CVE-2024-44308). In addition, malicious content can also be used for a cross-site scripting (XSS) attack (CVE-2024-44309).

These issues are being actively exploited in the wild. IGEL rates them as critical for IGEL OS 12, as Webkit is used to handle Single-Sign-On (SSO), and as high for OS 11.

Update Instructions

- OS 12: Update to the IGEL OS 12 base system app version 12.5.2 when it is available.
- OS 11: Update to IGEL OS 11.10.250 (planned for 25 February 2025)

References

- WSA-2024-0007: https://webkitgtk.org/security/WSA-2024-0007.html
- CISA KEV: https://www.cisa.gov/news-events/alerts/2024/11/21/cisa-adds-three-known-exploited-vulnerabilities-catalog

ISN 2024-22: Firefox ESR Vulnerabilities

Updated 9 January 2025 (OS 11.10.250 will contain fix)

First published 6 November 2024

CVSS 3.1: 8.2 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N

Summary

A security vulnerability has been found in the Firefox ESR web browser used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

It has been discovered that a permission leak is possible from a trusted site to an untrusted site via embed or object elements. This is rated as high and tracked as CVE-2024-10458.

Another high concern is the accessibility mode. When it is enabled, an attacker could cause a use-after-free, which leads to a crash that could potentially be exploited (CVE-2024-10459).

Update Instructions

- OS 12: Update to the IGEL OS app with Firefox ESR version 115.17 as soon as it is available from the IGEL App Portal.
- OS 11: Update to IGEL OS version 11.10.250 (planned for 25 February 2025).

References

- MFSA-2024-57: https://www.mozilla.org/en-US/security/advisories/mfsa2024-57/

ISN 2024-21: Chromium Critical Vulnerability

First published 5 November 2024

CVSS 3.1: 9.8 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

A critical security vulnerability has been found in the Chromium web browser used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

An out-of-bounds write has been found in Dawn, the WebGPU implementation in Chromium. It allows a remote attacker to write to memory out of bounds via a crafted HTML page. This is tracked as CVE-2024-10487 and rated critical.

In addition, a use-after-free has been discovered in the WebRTC component of Chromium. A remote attacker could potentially use it for heap corruption via an HTML page (CVE-2024-10488, high).

Update Instructions

- IGEL OS 12: Update to the IGEL OS app with Chromium version 130.0.6723.91 as soon as it is available from the IGEL App Portal.
- IGEL OS 11: Update to IGEL OS version 11.10.210 as soon as it is available.

References

- Chrome Releases Blog: https://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop_29.html

ISN 2024-20: Chromium Vulnerabilities

First published 23 October 2024

CVSS 3.1: 8.8 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

Important security vulnerabilities have been found in the Chromium web browser used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

Several type confusions have been found in the V8 JavaScript engine and rated high (CVE-2024-9602, CVE-2024-9603, CVE-2024-8638, CVE-2024-8904). In addition, inappropriate implementations exist in V8 (CVE-2024-9370, high, and CVE-2024-8905, medium).

Other vulnerabilities are use-after-free in the components Media Router (CVE-2024-8637, high) and Autofill (CVE-2024-8639, high) as well as an integer overflow in Layout (CVE-2024-7025, high) and a heap buffer overflow in Skia (CVE-2024-8636, high). In addition, there is insufficient data validation in Mojo (CVE-2024-9369, High).

Update Instructions

- OS 12: Update to the Chromium app with version 129.0.6668.100 as soon as it is available from the IGEL App Portal.
- OS 11: Update to IGEL OS version 11.10.190 as soon as it is available.

References

- Chrome Releases Blog: https://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop_8.html
- Chrome Releases Blog: https://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop.html
- Chrome Releases Blog: https://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop_17.html
- Chrome Releases Blog: https://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop_10.html

ISN 2024-19: CUPS Vulnerabilities

First published 31 October 2024

CVSS 3.1: 7.8 (High)

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Summary

Critical and high-security vulnerabilities have been found in CUPS 2.x, which is used in IGEL OS. These affect the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

CUPS is a standards-based, open-source printing system, and cups-filters provides backends, filters, and other software for CUPS 2.x to use on non-Mac OS systems.

In IGEL OS we are affected by CVE-2024-47177 : Any value passed to ‘FoomaticRIPCommandLine’ via a PPD file will be executed as a user-controlled command. However, we are not affected by the public exploit which utilizes CVE-2024-47176 as we don’t use 'cups-browsed' by default. As the attack chain is already interrupted by not using 'cups-browsed’ and remote protocol, CVE-2024-47175 is mitigated.

Update Instructions

- OS 12: Update to IGEL OS version 12.5.1 when available in November.
- OS 11: Update to IGEL OS version 11.10.210 available in November.

References

- CVE-2024-47177 https://nvd.nist.gov/vuln/detail/CVE-2024-47177
- CVE-2024-47175 https://nvd.nist.gov/vuln/detail/CVE-2024-47175
- CVE-2024-35235 https://nvd.nist.gov/vuln/detail/CVE-2024-35235
- CVE-2024-47176 https://nvd.nist.gov/vuln/detail/CVE-2024-47176
- CVE-2024-47076 https://nvd.nist.gov/vuln/detail/CVE-2024-47076

ISN 2024-18: Critical Firefox ESR Vulnerability

First published 15 October 2024

CVSS 3.1: 9.8 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

A critical security vulnerability has been found in the Firefox ESR web browser used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

A use-after-free vulnerability has been found in the Animation timelines component of Firefox. This could enable a remote attacker to execute code in the context of the content process. Mozilla has had reports that this issue is being exploited in the wild. It is tracked as CVE-2024-9680 and is rated critical.

Update Instructions

- OS 12: Update to the Firefox ESR app with version 115.16.1 as soon as it is available from the IGEL App Portal.
- OS 11: Update to IGEL OS version 11.10.190 as soon as it is available.

References

- CVE-2024-9680: https://www.cve.org/CVERecord?id=CVE-2024-9680
- MFSA2024-51: https://www.mozilla.org/en-US/security/advisories/mfsa2024-51/

ISN 2024-17: OpenSSH Vulnerability

First published 03 July 2024

CVSS 3.1: 9.0 (Critical)

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

Summary

A security vulnerability has been found in OpenSSH, a library for secure access to remote machines like IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

A signal handler race condition was found in OpenSSH. This could lead to unauthenticated remote code execution. The vulnerability is being tracked as CVE-2024-6387.

Mitigations

OpenSSH server functionality can be disabled by unchecking the profile setting System > Remote Access > SSH Access > Enable. Be aware that this disables SSH access to configured devices entirely.

Alternatively, SSH may be configured to LoginGraceTime = 0 by setting network.ssh_server.login_grace_time to 0 in the Registry. Do notice though that this enables trivial Denial-of-Service (DoS) of SSH connections because only one authentication attempt is accepted at once.

Update Instructions

- OS 12: Update to base system version 12.4.2 (expected July 18th)
- OS 11: Update to the IGEL OS 11.10.150 (expected July 11th)

References

- OpenSSH project release notes: https://www.openssh.com/txt/release-9.8
- Qualys Vulnerability write-up: qualys.com/2024/07/01/cve-2024-6387/regresshion.txt[13]
- NVD: https://nvd.nist.gov/vuln/detail/CVE-2024-6387

13. http://qualys.com/2024/07/01/cve-2024-6387/regresshion.txt

ISN 2024-16: Libarchive Vulnerability

First published 20 June 2024

CVSS 3.1: 7.8 (High)

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

A security vulnerability has been found in Libarchive, a library for compressing and decompressing files used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

Libarchive contains a heap-based buffer overflow that can lead to remote code execution (RCE). It is tracked as CVE-2024-26256 and rated high.

Update Instructions

- OS 12: Update to base system version 12.4.2 or newer.
- OS 11: Update to the IGEL OS 11.10.150 or newer.

References

- CVE-2024-26256: https://www.cve.org/CVERecord?id=CVE-2024-26256

ISN 2024-15: Libaom Vulnerability

First published 20 June 2024

CVSS 3.1: 8.4 (High)

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

A security vulnerability has been found in the Libaom multimedia library used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

Libaom contains an integer overflow in the internal function img_alloc_helper, which can lead to a heap buffer overflow. Also, calling it with large values may lead to further integer overflows in calculations. This may lead to arbitrary code execution and is rated as high (CVE-2024-5171).

Update Instructions

- OS 12: Update to base system version 12.4.2 or newer.
- OS 11: Update to the upcoming IGEL OS 11.10.150 or newer.

References

- CVE-2024-5171: https://www.cve.org/CVERecord?id=CVE-2024-5171

ISN 2024-14: Chromium Vulnerabilities

First published 18 June 2024

CVSS 3.1: 8.8 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

Multiple security vulnerabilities have been found in the Chromium web browser used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

Type confusions have been discovered in the JavaScript engine V8 (CVE-2024-4947and CVE-2024-5274). They are rated high and could allow a remote attacker to execute arbitrary code. Google is aware that exploits for both these issues exist in the wild.

Furthermore, Google reports heap buffer overflows in ANGLE (CVE-2024-5159, high) and Dawn (CVE-2024-5160, high) as well as occurrences of use-after free in Dawn (CVE-2024-4948, high) and Scheduling (CVE-2024-5157, high).

Update Instructions

- OS 12: Update to the Chromium app version 125.0.6422.112 or newer from the App Portal.
- OS 11: Update to the upcoming IGEL OS 11.10.150.

References

- Chrome Releases Blog: https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_23.html
- Chrome Releases Blog: https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_21.html
- Chrome Releases Blog: https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_15.html

ISN 2024-13: Firefox ESR Vulnerabilities

First published 18 June 2024

CVSS 3.1: 7.5 (high)

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

Multiple security vulnerabilities have been found in the Firefox ESR web browser used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

A vulnerability has been discovered in PDF.js, the component Firefox uses to render PDF files: JavaScript embedded into the PDF document is executed in the context of the hosting domain (CVE-2024-4367, high). In IGEL OS 11 this is already mitigated by the fact that Firefox ESR opens PDF files in the external PDF viewer, but the Firefox ESR App for OS 12 is fully affected.

Further issues rated high were found in the JIT component: GetBoundName returning the wrong object (CVE-2024-3852), an out-of-bounds-read occurring after a mis-optimized switch statement (CVE-2024-3854), and potential use-after-free crashes during garbage collection (CVE-2024-3857). Additionally, a memory safety bug came to light, which showed evidence of memory corruption and could potentially be exploited to run arbitrary code (CVE-2024-3864, high).

Update Instructions

- OS 12: Update to the Firefox ESR app version 115.11 or newer when it is available in the App Portal.
- OS 11: Update to the upcoming IGEL OS 11.10.150.

References

- MFSA 2024-22: https://www.mozilla.org/en-US/security/advisories/mfsa2024-22/
- Github-reviewed Advisory for CVE-2024-4367: https://github.com/advisories/GHSA-wgrm-67xf-hhpq
- MFSA 2024-19: https://www.mozilla.org/en-US/security/advisories/mfsa2024-19/

ISN 2024-12: Vulnerability in Starter License Verification

First published 15 May 2024

CVSS 3.1: 7.8 (high)

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Summary

A security vulnerability has been found in the Starter License verification mechanism in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

An issue in the code verifying the validity of the Starter License can enable a local attacker to execute arbitrary commands as a non-privileged user. This vulnerability is rated as high.

IGEL would like to thank Zack Didcott for coordinated disclosure.

Update Instructions

- OS 12: Update to version 12.4.0 of the IGEL OS 12 base system.
- OS 11: Update to IGEL OS version 11.10.100.

References

- CWE-427: Uncontrolled Search Path Element: https://cwe.mitre.org/data/definitions/427.html

ISN 2024-11: Chromium Critical Vulnerability

First published 30 April 2024

CVSS 3.1: n/a (critical)

CVSS:3.1 n/a

Summary

Multiple security vulnerabilities have been found in the Chromium web browser used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

A type confusion in ANGLE, the WebGL component in Chromium, is rated as a critical vulnerability (CVE-2024-4058). In addition, issues rated high exist: An out-of-bounds read in the V8 JavaScript engine API (CVE-2024-4059) and a use-after-free in the WebGPU implementation Dawn (CVE-2024-4060).

Update Instructions

- OS 12: Update to the OS 12 Chromium app version 124.0.6367.78 or newer when it is available in the IGEL App Portal.
- OS 11: Update to OS 11.10.100 when it is available (mid-May)

References

- Chrome Releases Blog: https://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop_24.html

ISN 2024-10: Chromium Critical Vulnerability

Updated 25 April 2024 (Chromium App 124.0.6367.60 available)

First published 15 April 2024

CVSS 3.1: 9.8 (critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P

Summary

Multiple security vulnerabilities have been found in the Chromium web browser used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

Among the issues discovered is a use-after-free in ANGLE, the WebGL component in Chromium. An attacker could abuse it to exploit heap corruption via a crafted HTML page, so this is rated as critical (CVE-2024-2883). Google is aware that an exploit for this vulnerability exists in the wild.

Apart from that, issues rated high have been found: A use-after-free in Dawn (CVE-2024-2885), a use-after-free in WebCodecs (CVE-2024-2886) and a type confusion in WebAssembly (CVE-2024-2887).

Update Instructions

- OS 12: Update to the OS 12 Chromium app version 124.0.6367.60 from the IGEL App Portal.
- OS 11: The IGEL OS Private Build 11.09.268 with Chromium updated to version 123.0.6312.105 is available from IGEL Customer Engineering.

References

- CVE-2024-2883: https://www.cve.org/CVERecord?id=CVE-2024-2883
- Chrome Releases Blog: https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_26.html

ISN 2024-09: Xdg-open “Open With” Vulnerability

First published 15 May 2024

CVSS 3.1: 7.8 (high)

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Summary

A security vulnerability has been found in the Xdg-open utility used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

A security vulnerability has been discovered in the Xdg-open utility (“Open with …”) in the context of IGEL OS. It can be used by a local attacker to execute arbitrary commands. This issue is rated as high.

IGEL has patched Xdg-open to remediate this issue, which specifically occurs in the IGEL OS Desktop context.

Update Instructions

- OS 12: Update to the OS 12 base system version 12.3.2 or newer.
- OS 11: Update to IGEL OS version 11.10.100.

References

- Xdg-open: https://portland.freedesktop.org/doc/xdg-open.html

ISN 2024-08: Firefox ESR Vulnerabilities

First published 26 March 2024

CVSS 3.1: 9.8 (critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

Multiple security vulnerabilities have been found in the Firefox ESR web browser used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

Among the vulnerabilities found, one is rated as critical: An attacker might be able to inject an event handler into a privileged object, which may enable them to execute arbitrary code (CVE-2024-29944).

Apart from that, several issues rated as high have been identified. Several methods could have experienced integer overflows, causing underallocation of an output buffer, and leading to an out-of-bounds write (CVE-2024-2608). An out-of-bounds memory read was discovered in networking channels (CVE-2024-1546). ICU can be affected by resource exhaustion (CVE-2024-2616), and a TLS method in NSS can cause a potentially exploitable crash (CVE-2024-0743). Another issue enables an attacker to spoof an alert dialog on another site (CVE-2024-1547). Memory safety bugs conclude the list (CVE-2024-1553, CVE-2024-2614).

Update Instructions

- OS 12: Update the OS 12 Firefox ESR App to version 115.9.1 when it is available on the IGEL App Portal.
- OS 11: Update to IGEL 11.09.310 when it is available.

References

- MSFA-2024-16: https://www.mozilla.org/en-US/security/advisories/mfsa2024-16/
- MSFA-2024-12: https://www.mozilla.org/en-US/security/advisories/mfsa2024-13/
- MSFA-2024-06: https://www.mozilla.org/en-US/security/advisories/mfsa2024-06/

ISN 2024-07: Chromium Vulnerabilities

Updated 15 April 2024 (IGEL OS 11.09.310 available)

First published 25 March 2024

CVSS 3.1: 8.8 (high)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

Multiple security vulnerabilities have been found in the Chromium web browser used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

Out of the security issues found in the Chromium web browser, several affect the V8 JavaScript engine. They are all rated high and range from type confusion (CVE-2024-0518, CVE-2024-1938, CVE-2024-1939) over inappropriate implementation (CVE-2024-2174) to out-of-bounds memory access (CVE-2024-2173, CVE-2024-0519).

Use-after-free vulnerabilities rated high have been found in the Mojo (CVE-2024-1284, CVE-2024-1670), Performance Manager (CVE-2024-2400), WebAudio (CVE-2024-0807), Network (CVE-2024-1077), WebRTC (CVE-2024-1059), Canvas (CVE-2024-1060) and FedCM (CVE-2024-2176) components of the browser. These could allow a remote attacker to exploit heap corruption via crafted data.

Further issues are out-of-bounds memory access in Blink (CVE-2024-1669), heap buffer overflow in Skia (CVE-2024-1283), an inappropriate implementation in Accessibility (CVE-2024-0812) and an Integer underflow in WebUI (CVE-2024-0808). These are also rated high.

Update Instructions

- OS 12: Update the OS 12 Chromium App to version 122.0.6261.128 when it is available on the IGEL App Portal.
- OS 11: Update to IGEL OS version 11.09.310.

References

- Chrome Releases Blog: https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_12.html
- Chrome Releases Blog: https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop.html
- Chrome Releases Blog: https://chromereleases.googleblog.com/2024/02/stable-channel-update-for-desktop_27.html
- Chrome Releases Blog: https://chromereleases.googleblog.com/2024/02/stable-channel-update-for-desktop_20.html

- Chrome Releases Blog: https://chromereleases.googleblog.com/2024/02/stable-channel-update-for-desktop_13.html
- Chrome Releases Blog: https://chromereleases.googleblog.com/2024/02/stable-channel-update-for-desktop.html
- Chrome Releases Blog: https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_30.html
- Chrome Releases Blog: https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html
- Chrome Releases Blog: https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_16.html

ISN 2024-06: OS 11 Kernel Vulnerabilities

First published 12 March 2024

CVSS 3.1: 8.4 (High)

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

Multiple security vulnerabilities have been found in the Linux Kernel version used in IGEL OS. This affects the following IGEL products:

- IGEL OS 11

Details

The Linux Kernel version 6.1.42 used in IGEL OS 11 is affected by a use-after-free vulnerability in the NVMe/TCP subsystem in the Linux kernel. This may allow an attacker to cause a use-after-free and double-free problem, which may permit remote code execution or lead to local privilege escalation (CVE-2023-5178, high).

Another security issue has been discovered in the TLS subsystem of the Linux Kernel. Under certain circumstances, a use-after-free can be triggered (CVE-2024-26582). An attacker could use this to trigger a denial of service or code execution, so the severity of this vulnerability is rated as high. CVE-2024-0646 also affects TLS and may lead to privilege escalation. Both issues are rated as high.

Improper access control has been found in the Intel Ethernet Controller RDMA driver for Linux before version 1.9.30. It may allow an unauthenticated user to potentially enable escalation of privilege via network access (CVE-2023-25775, high).

Several vulnerabilities affect the kernel's net/sched subsystem and can allow for local privilege escalation (CVE-2023-4206, CVE-2023-4207, CVE-2023-4208, CVE-2023-4623 and CVE-2023-4921).

Netfilter/nftables-is affected by CVE-2023-6817, CVE-2024-1086, CVE-2023-4015, CVE-2023-4147, CVE-2023-42753 and CVE-2024-22705, which might enable privilege escalation.

CVE-2023-40283 and CVE-2023-51779 both describe use-after-frees in Bluetooth.

In addition to the above, the kernel is affected by the issues CVE-2023-46813, CVE-2023-5717, CVE-2023-6932, CVE-2023-6531, CVE-2023-6931, CVE-2023-51780, CVE-2023-51781 and CVE-2023-51782. They are rated as high and may lead to local privilege escalation.

Update Instructions

- OS 11: Update to IGEL OS 11.10.100, which has a complete kernel upgrade, when it is available.

References

- CVE-2023-5178: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5178
- CVE-2024-26582: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26582
- CVE-2024-0646: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-0646

- CVE-2023-25775: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25775
- CVE-2023-4206: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4206
- CVE-2023-4207: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4207
- CVE-2023-4208: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4208
- CVE-2023-4623: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4623
- CVE-2023-4921: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4921
- CVE-2023-6817: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-6817
- CVE-2024-1086: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-1086
- CVE-2023-4015: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4015
- CVE-2023-4147: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4147
- CVE-2023-42753: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42753
- CVE-2024-22705: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-22705
- CVE-2023-40283: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40283
- CVE-2023-51779: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-51779
- CVE-2023-46813: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-46813
- CVE-2023-5717: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5717
- CVE-2023-6932: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-6932
- CVE-2023-6531: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-6531
- CVE-2023-6931: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-6931
- CVE-2023-51780: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-51780
- CVE-2023-51781: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-51781
- CVE-2023-51782: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-51782

ISN 2024-05: OS 12 Kernel Vulnerability

First published 8 March 2024

CVSS 3.1: 8.4 (High)

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

A security vulnerability has been found in the Linux Kernel used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12

Details

A security issue has been discovered in TLS subsystem of the Linux Kernel. Under certain circumstances, a use-after-free can be triggered (CVE-2024-26582). An attacker could use this to trigger a denial of service or code execution, so the severity of this vulnerability is rated as high.

Update Instructions

- OS 12: IGEL is preparing a fixed OS 12 base system version.

References

- CVE-2024-26582: https://cve.org/CVERecord/?id=CVE-2024-26582

ISN 2024-04: Libuv Vulnerability

First published 4 March 2024

CVSS 3.1: 7.3 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Summary

A security vulnerability has been found in the Libuv library used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12 (only if Firefox app is installed)
- IGEL OS 11

Details

A security issue has been discovered in the `uv_getaddrinfo` function in Libuv. It truncates hostnames to 256 characters before it calls `getaddrinfo`. An attacker could exploit this to create payloads that are resolved to unintended IP addresses, thus bypassing security checks.

The OS 12 base system contains Libuv, but the library is only used if the Firefox app is installed.

Update Instructions

- OS 12: Update to OS 12 base system version 12.4.1 when it is available.
- OS 11: IGEL is working on an OS 11 release with an updated Libuv.

References

- CVE-2024-24806: https://www.cve.org/CVERecord?id=CVE-2024-24806

ISN 2024-03: Firefox ESR Vulnerabilities

First published 31 January 2024

CVSS 3.1: 8.8 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

Multiple security vulnerabilities have been found in the Firefox ESR web browser used in IGEL OS. This affects the following IGEL products:

- IGEL OS 11

Details

The WebGL DrawElementsInstanced method in Firefox ESR is susceptible to a heap buffer overflow when used on systems with the Mesa VM driver (typically used when running on VMware virtualization). This issue is rated high, as it could allow an attacker to perform remote code execution and sandbox escape (CVE-2023-6856). Additionally, ownership mismanagement leads to a use-after-free in ReadableByteStreams that is also rated as high (CVE-2023-6207).

Apart from that, multiple memory management vulnerabilities have been found that are rated as medium.

Update Instructions

- IGEL OS 11: IGEL is preparing an IGEL OS 11 release with an updated Firefox ESR version.

References

- https://nvd.nist.gov/vuln/detail/CVE-2023-6856
- https://nvd.nist.gov/vuln/detail/CVE-2023-6207
- https://www.mozilla.org/en-US/security/advisories/mfsa2024-02/
- https://www.mozilla.org/en-US/security/advisories/mfsa2023-54/
- https://www.mozilla.org/en-US/security/advisories/mfsa2023-50/

ISN 2024-02: X.org Vulnerabilities

First published 31 January 2024

CVSS 3.1: 7.8 (High)

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Summary

Multiple security vulnerabilities have been found in the X.org display system used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

It has been discovered that the X Server incorrectly handled memory when processing the DeviceFocusEvent and ProcXIQueryPointer APIs (CVE-2023-6816). This could lead the X server to crash, reveal sensitive information, or allow the execution of arbitrary code. This is rated as high. The server may also handle reattaching to a different master device incorrectly, potentially leading to a crash or code execution (CVE-2024-0229, high).

Mitigation

To prevent these vulnerabilities from being exploited remotely, disable X11 forwarding over SSH (see instructions below). However, this does not defend against local threats.

- IGEL OS 12: In the Profile Configurator or the Device Configurator, go to **System > Remote Access > SSH Access** and make sure that **Permit X11 forwarding** is disabled. By default, this service is disabled. Please note that X 11 forwarding, like the other SSH access settings, is only effective if the **Enable** parameter is activated.
- IGEL OS 11: Disable X11 forwarding, see *IGEL OS 11.10 > IGEL OS Articles > Security > Securing IGEL OS Endpoints > Configuring Remote Access and Management > Disabling X11 Forwarding*.

Additionally, leave TCP connections for X11 disabled:

- IGEL OS 12: Leave **User Interface > Display Settings > Access Control > Disable TCP connections** as it is or reset it to default.
- IGEL OS 11: Leave **User Interface > Display > Access Control > Disable TCP connections** as it is or reset it to default.

Update Instructions

- IGEL OS 12: IGEL is preparing an updated IGEL OS 12 Base System app.
- IGEL OS 11: IGEL is preparing an updated IGEL OS 11 release.

References

- CVE-2023-6816: https://cve.mitre.org/cgi-bin/cvename.cgi?name=2023-6816
- CVE-2024-0229: https://cve.mitre.org/cgi-bin/cvename.cgi?name=2024-0229
- CVE-2024-21885: https://cve.mitre.org/cgi-bin/cvename.cgi?name=2024-21885
- CVE-2024-21886: https://cve.mitre.org/cgi-bin/cvename.cgi?name=2024-21886

ISN 2024-01: Chromium Vulnerabilities

First published 22 January 2024

CVSS 3.1: 8.8 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

Multiple Security vulnerabilities have been discovered in the Chromium web browser used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

Several memory management issues have been found and rated high: a use after free (CVE-2024-0222) and a heap buffer overflow in ANGLE (High CVE-2024-0223), a use after free in WebAudio (CVE-2024-0224), and a use after free in WebGPU (CVE-2024-0225). Additionally, there is insufficient data validation in Extensions (CVE-2024-0333), which is also rated as high.

Update Instructions

- OS 12: Upgrade to the OS 12 Chromium App version 120.0.6099.216 as soon as it is available from the IGEL App Portal.
- OS 11: Upgrade to OS 11.09.210.

References

- https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_9.html
- https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop.html

ISN 2023-39: SSH Terrapin Vulnerability

First published 5 February 2024

CVSS 3.1: 5.9 (Medium)

CVSS:3.1/AV:N/AC:H/PR:N/S:U/C:N/I:H/A:N

Summary

A security vulnerability has been discovered in secure shell (SSH), which is used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

A vulnerability has been found in the SSH protocol that weakens the secure channel, so that messages could be removed during transmission.

However, an attack is only possible if the attacker can man-in-the-middle the SSH traffic and if the connection uses either **ChaCha20-Poly1305** or a **CBC cipher with Encrypt-then-MAC (CVE-2023-48795)**.
This is why this vulnerability is rated as medium.

It affects the OpenSSH server as well as the client.

Mitigation

OS 12

- The OpenSSH server in OS 12 is not activated by default. SSH is not necessary for managing IGEL OS, so unless you have another use case you can leave it deactivated.
- If you use OS 12 base system version 12.3.1, you have the latest OpenSSH 9.6p1. When you use this version or newer on the peer, they will automatically use the new "strict KEX" protocol extension.

OS 11

- The OpenSSH server in OS 11 is active by default, but SSH is not necessary for managing IGEL OS. Unless you have another use case, deactivate it.
- If you use IGEL OS 11.09.210, you have the latest OpenSSH 9.6p1. When you use this version or newer on the peer, they will automatically use the new "strict KEX" protocol extension.

Update Instructions

- OS 12: Update to OS 12 base system version **12.3.1 or newer**, which has OpenSSH version 9.6p1.

- OS 11: Update to IGEL OS version **11.09.210 or newer**, which has OpenSSH version 9.6p1.

References

- Terrapin Attack: https://terrapin-attack.com

ISN 2023-38: X.org Vulnerabilities

Updated 22 January 2024 (fixed versions)

First published 19 December 2023

CVSS 3.1: 7.8 (High)

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Summary

Security vulnerabilities have been discovered in the X.org graphics system used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

A flaw was found in xorg-server. Querying or changing XKB button actions such as moving from a touchpad to a mouse can result in out-of-bounds memory reads and writes. This may allow local privilege escalation or possible remote code execution (RCE) in cases where X11 forwarding is involved. This is tracked as CVE-2023-6377 and rated as high.

Additionally, a specially crafted request to RRChangeProviderProperty or RRChangeOutputProperty can trigger an integer overflow which may lead to a disclosure of sensitive information (CVE-2023-6478, high).

Mitigation

Remote code execution can be mitigated by disabling X11 forwarding over SSH (see instructions below). However, this does not fix the local threats.

- OS 12: Disable X11 forwarding in Setup under **System > Remote Access > SSH Access**, if the SSH services is active – by default this service is disabled.
- OS 11: Disable X11 forwarding, see *IGEL OS 11.10 > IGEL OS Articles > Security > Securing IGEL OS Endpoints > Configuring Remote Access and Management > Disabling X11 Forwarding*.

Update Instructions

- OS 12: Update to OS 12 base system version 12.3.1 (planned for 6 February) or newer.
- OS 11: Update to IGEL OS version 11.09.210 or newer.

References

- CVE-2023-6377: https://cve.mitre.org/cgi-bin/cvename.cgi?name=2023-6377
- CVE-2023-6478: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-6478

ISN 2023-36: BlueZ Vulnerability

Updated 23 January 2024 (corrected OS 11 update)

Updated 16 January 2024 (added fixed versions)

First published 19 December 2023

CVSS 3.1: 8.8 (High)

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

A security vulnerability has been discovered in the Bluetooth stack used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

It has been found that BlueZ does not properly restrict non-bonded devices from injecting Human Interface Device (HID) events into the input subsystem. This could allow a physically proximate attacker to inject keystrokes and mouse events – and execute arbitrary commands when the device is discoverable.

Mitigation

1. Use wired USB devices for keyboard and mouse.
2. Disable Bluetooth in Setup **Devices > Bluetooth**.

Update Instructions

- OS 12: Update to OS 12 base system app version 12.3.1 (planned to be released on 6 Feb 2024).
- OS 11: IGEL is preparing an OS 11 release with fixed Bluetooth.

References

- CVE-2023-45866: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-45866

ISN 2023-35: GIMP Vulnerabilities

First published 22 January 2023

CVSS 3.1: 8.2 (High)

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Summary

Multiple security vulnerabilities have been discovered in the GIMP image processing library used in IGEL OS. This affects the following IGEL products:

- IGEL OS 11 (not in the default configuration)

Details

GIMP is vulnerable to crafted files in several formats: Processing DDS, PSP or PSD files can cause overflows and enable remote code execution (CVE-2023-44441, CVE-2023-44442, CVE-2023-44443). This is rated as high. Crafted XCF files can exhaust memory or trigger an unhandled exception, which may lead to a denial of service (CVE-2022-30067, CVE-2022-32990), which is rated as medium.

Mitigation

GIMP is not active in the IGEL OS 11 default configuration. It is only mounted if you activate **Scanner Support / SANE (Limited Support ...)** in **System > Firmware Customization > Features** in Setup. If you have it activated, you can deactivate it to mitigate this vulnerability.

Update Instructions

- OS 11: Update to IGEL OS version 11.09.210 or newer

References

- CVE-2023-44441: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44441
- CVE-2023-44442: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44442
- CVE-2023-44443: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44443
- CVE-2023-44444: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44444
- CVE-2022-30067: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30067
- CVE-2022-32990: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32990

ISN 2023-34: Perl Vulnerabilities

First published 19 December 2023

CVSS 3.1: 8.4 (High)

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

A security vulnerability has been discovered in the Perl scripting language used in IGEL OS. This affects the following IGEL products:

- IGEL OS 11

Details

Perl is vulnerable to a stack-based crash that can lead to remote code execution or local privilege escalation (CVE-2022-48522). This is rated as high. Additionally, when a regular expression is compiled by Perl, an attacker could craft an expression that leads to a controlled overflow in a heap allocated buffer (CVE-2023-47038, high).

Update Instructions

- OS 11: Update to IGEL OS 11.09.160 when available.

References

- CVE-2022-48522: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE- CVE-2022-48522[14]
- CVE-2023-47038: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-47038

14. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-%20CVE-2022-48522

ISN 2023-33: Zlib Vulnerability

First published 18 December 2023

CVSS 3.1: 9.8 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

A security vulnerability has been found in the Zlib compression library used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

The MiniZip component in Zlib contains an integer overflow and resultant heap-based buffer overflow via a long filename, comment, or extra field. This could enable an attacker to execute arbitrary code via constructed input. This vulnerability is tracked as CVE-2023-45853 and rated critical.

Update Instructions

- OS 12: Update to IGEL OS version 12.2.2 PR (Patch Release) 2 or 12.3.0 when available.
- OS 11: Update to IGEL OS version 11.09.160 when available.

References

- CVE-2023-45853: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-45853

ISN 2023-32: Chromium Vulnerabilities

Updated 16 January 2024 (fixed versions)

First published 12 December 2023

CVSS 3.1: 8.3 (High)

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H/E:F

Summary

Multiple security vulnerabilities have been found in the Chromium web browser used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

An integer overflow has been found in Chromium's 2D graphics library Skia that could allow a remote attacker to escape the sandbox via a malicious file. Google reports that there is an exploit for this issue being used in the wild, and the vulnerability is rated as high (CVE-2023-6345). Also, six further issues rated high have been reported that concern memory management vulnerabilities.

Update Instructions

- OS 12: An updated Chromium app is available from the IGEL App Portal.
- OS 11: Update to private build 11.09.151, which is available on request from IGEL Support or to IGEL OS 11.09.160, which is publicly available.

References

- CVE-2023-6345: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-6345
- Google Chrome Releases: Stable Channel Update for Desktop: https://chromereleases.googleblog.com/2023/11/stable-channel-update-for-desktop_28.html

ISN 2023-31: Webkit Vulnerabilities

Updated 11 January 2024 (corrected OS 12 fix version)

First published 22 November 2023

CVSS 3.1: 8.8 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

Security vulnerabilities have been found in the Webkit browser engine used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

A vulnerability in Webkit allows a remote attacker to potentially execute arbitrary code using web content. This is tracked as CVE-2023-42852 and rated high. As second issue can lead to denial of service and is also triggered by web content (CVE-2023-41983, medium).

Update Instructions

- OS 12: Update to base system app version 12.3.1 (available 6 February)
- OS 11: Update to version 11.09.150 (available 6 December)

References

- CVE-2023-42852: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42852
- CVE-2023-41983: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41983

ISN 2023-30: Ffmpeg Vulnerabilities

First published 22 November 2023

CVSS 3.1: 8.8 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

Security vulnerabilities have been found in the Ffmpeg video library used in IGEL OS. This affects the following IGEL products:

- IGEL OS 11

Details

Several vulnerabilities have been identified in the Ffmpeg multimedia framework (CVE-2022-4907). They could allow an attacker to cause denial of service or potentially execute arbitrary code. These vulnerabilities are rated as high.

Update Instructions

- OS 11: Update to version 11.09.150 (available 6 December)

References

- CVE-2022-4907: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-4907

ISN 2023-29: Chromium Vulnerabilities

First published 9 November 2023

CVSS 3.1: 8.8 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

Multiple vulnerabilities have been discovered in the Chromium web browser which is used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

Chromium has been found to contain an inappropriate implementation in the Payments component that allows a remote attacker to bypass XSS preventions via a malicious file. This is tracked as CVE-2023-5480 and rated as high. In Chromium's USB component insufficient data validation (CVE-2023-5482, high) could allow out of bounds memory access via a crafted HTML page. Additionally, an integer overflow has been reported in USB that could be used to exploit heap corruption via a crafted web page (CVE-2023-5849, high).

Update Instructions

- OS 12: IGEL is preparing an updated OS 12 Chromium app.
- OS 11: IGEL is preparing an updated OS 11 version with an updated Chromium.

References

- CVE-2023-5480: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5480
- CVE-2023-5482: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5482
- CVE-2023-5849: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5849

ISN 2023-28: Firefox ESR Vulnerabilities

Updated 16 January 2024 (added fixed version)

First published 9 November 2023

CVSS 3.1: 7.5 (High)

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

Multiple vulnerabilities have been discovered in the Firefox ESR web browser which is used in IGEL OS. This affects the following IGEL products:

- IGEL OS 11

Details

It has been found that it is possible for certain Firefox prompts and dialogs to be activated or dismissed unintentionally by the user due to an insufficient activation-delay (CVE-2023-5721). This vulnerability is rated as high. Apart from that, there are memory safety bugs which could lead to memory corruption and could be abused to run arbitrary code (CVE-2023-5730, high).

Update Instructions

- OS 11: Update to IGEL OS version 11.09.150 or newer.

References

- CVE-2023-5721: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5721
- CVE-2023-5730: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5730

ISN 2023-27: ActiveMQ in UMS HA

First published 3 November 2023

CVSS 3.1: 10.0 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:H

Summary

Apache ActiveMQ is vulnerable to a critical remote code execution vulnerability. This vulnerability affects the High Availability (HA) feature **only**, used in UMS in the following versions:

- UMS versions <= 12.02.120

Details

Apache ActiveMQ is vulnerable to a critical (10.0) remote code execution vulnerability being tracked with CVE-2023-46604. The vulnerability may allow a remote attacker with network access to a broker to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause the broker to instantiate any class on the classpath. Rapid7 has confirmed the public exploit and are investigating the activity of the HelloKitty ransomware group exploiting this vulnerability.

Update Instructions

- UMS 12: We are preparing an emergency release of UMS 12.02.130.
- UMS 6: Upgrade to UMS 12.02.130, available soon.

References

- CVE-2023-46604: https://nvd.nist.gov/vuln/detail/CVE-2023-46604
- Apache advisory: https://activemq.apache.org/security-advisories.data/CVE-2023-46604-announcement.txt
- Report from Rapid7 confirming public exploitation attempts and PoC: https://www.rapid7.com/blog/post/2023/11/01/etr-suspected-exploitation-of-apache-activemq-cve-2023-46604/

ISN 2023-26: X.org Vulnerabilities

Updated 27 November 2023 (Update Instructions)

First published 9 November 2023

CVSS 3.1: 7.8 (High)

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Summary

Multiple vulnerabilities have been discovered in the X.org display server, which is used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

The X.org server has been found to have three local vulnerabilities. CVE-2023-5367 is an out-of-bounds write flaw in xorg-x11-server that could be used to crash the server or escalate the attacker's privileges. It is rated as high. CVE-2023-5574 tracks a vulnerability in Xvfb, also rated as high, that could have the same effect. Finally, CVE-2023-5380 is a use-after-free flaw in the xorg-x11-server that could crash the server in a very specific scenario (medium).

Update Instructions

- OS 12: Update to OS 12 base system app version 12.2.2.
- OS 11: Update to OS 11.09.150 (available 6 December).

References

- Org Security Advisory: https://lists.x.org/archives/xorg-announce/2023-October/003430.html
- CVE-2023-5367: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5367
- CVE-2023-5574: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5574
- CVE-2023-5380: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2023-5380

ISN 2023-24: Chromium Vulnerability

Updated 24 October 2023 (OS 11.09.110 available)

First published 13 October 2023

CVSS 3.1: 8.8 (High)

CVSS:3.1 /AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

A security vulnerability has been found in the Chromium web browser. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

Google has reported a high vulnerability in Chromium (CVE-2023-5218). It is a use-after-free in the Site Isolation component, which could enable an attacker to execute arbitrary code via a crafted HTML page.

Update Instructions

- OS 12: IGEL is preparing an updated Chromium app for OS 12.
- OS 11: Update to IGEL OS 11.09.110 or newer.

References

- Chrome Blog Stable Channel Update for Desktop: https://chromereleases.googleblog.com/2023/10/stable-channel-update-for-desktop_10.html
- CVE-2023-5218: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5218

ISN 2023-23: Curl Vulnerability

Updated 2 November 2023 (OS 12.2.1 available)

First published 12 October 2023

CVSS 3.1: 7.5 (High)

CVSS:3.1: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

A vulnerability has been found in the Curl package, which is used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

A heap-based buffer overflow was found in the SOCKS5 proxy handshake in the Curl package. This vulnerability rated high is being tracked with CVE-2023-38545. In the updated packages they also resolved a low severity vulnerability for libcurl which is tracked with CVE-2023-38546. These vulnerabilities were responsibly disclosed to the Curl maintainers and there is no evidence of it being exploited before.

Update Instructions

- OS 12: Update to IGEL OS 12.2.1 or newer.
- OS 11: Update to IGEL OS 11.09.110 or newer.

References

- Curl security advisory: https://curl.se/docs/CVE-2023-38545.html
- Details of disclosure: https://hackerone.com/reports/2187833

ISN 2023-22: Multiple X11 Vulnerabilites

Updated 17 October 2023 (IGEL OS 11.09.100 available)

First published 6 October 2023

CVSS 3.1: 5.5 (Medium)

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A

Summary

Multiple issues have been found in the libX11 and libXpm libraries published by X.Org, which are used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

The first issue (CVE-2023-43785) can be triggered by connecting to an X server that sends specially crafted replies to X11 protocol requests – this can happen with an X Session from IGEL OS. It can lead to an out-of-bounds memory access and is rated as medium.

The other four issues (CVE-2023-43786, CVE-2023-43787, CVE-2023-43788 and CVE-2023-43789) can be triggered by opening specially crafted XPM format image files via libXpm and can exhaust the stack, lead to a heap overflow or cause an out-of-bounds read. They are all rated as medium.

Update Instructions

- OS 12: IGEL is preparing an updated Base system for OS 12.
- OS 11: Update to IGEL OS 11.09.100 or newer.

References

- X.Org Security Advisory: Issues in libX11 prior to 1.8.7 & libXpm prior to 3.5.17 - https://lists.x.org/archives/xorg/2023-October/061506.html

ISN 2023-21: Libvpx Vulnerability in Chromium and Firefox

Updated 24 October 2023 (OS 11.09.110 available)

First published 5 October 2023

CVSS 3.1: 8.8 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

A vulnerability has been found in the Libvpx video library. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

A vulnerability rated high (CVE-2023-5217) has been found in the code for the VP8 video format in Libvpx. This library is used in the Chromium and Firefox web browsers. A remote attacker could potentially exploit heap corruption via a crafted HTML page. Google and Mozilla report that this vulnerability is being used in the wild.

Mitigation

- OS 11: If feasible, use Firefox as your web browser and add the following custom command to **System > Firmware Customization > Custom Commands > Base > Initialization** in order to filter out media that could be used for an attack:

```
FFPREFS=/services/fbrw/bin/firefox_preferences
cp -v $FFPREFS ${FFPREFS}_bin
cat > $FFPREFS <<"EOF"
#!/bin/bash
/services/fbrw/bin/firefox_preferences_bin "$@"
echo 'user_pref("image.webp.enabled", false);
user_pref("media.ffvpx.enabled", false);
user_pref("media.ffvpx.mp3.enabled", false);
user_pref("media.ffvpx.opus.enabled", false);
user_pref("media.ffvpx.vorbis.enabled", false);
```

```
user_pref("media.ffvpx.wav.enabled", false);' >> ~user/.mozilla/firefox/browser0/user.js
EOF
```

Update Instructions

- OS 12: IGEL is preparing an updated Chromium app for OS 12.
- OS 11: Update to IGEL OS 11.09.110 or newer.

References

- CVE-2023-5217: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5217

ISN 2023-20: Firefox Libwebp Vulnerability

Updated 27 September 2023 (fix version, add CVE-2023-5129)

First published 14 September 2023

CVSS 3.1: 10.0 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Summary

A critical vulnerability has been found in the Firefox web browser. This affects the following IGEL products:

- IGEL OS 11

Details

A zero-day critical heap buffer overflow vulnerability has been found in the WebP library used by Firefox. This vulnerability can be tracked with CVE-2023-4863 and CVE-2023-5129. Apple's Security Engineering and Architecture (SEAR) and The Citizen Lab are not publishing the details of this vulnerability as it has been seen exploited in-the-wild and they are giving time for people to update their browsers.

Update Instructions

- OS 11: Update to IGEL OS 11.09.100 (planned for 5 October 2023) with an updated Firefox.

References

- CVE-2023-4863 - https://nvd.nist.gov/vuln/detail/CVE-2023-4863
- CVE-2023-5129 - https://nvd.nist.gov/vuln/detail/CVE-2023-5129
- Mozilla's advisory - https://www.mozilla.org/en-US/security/advisories/mfsa2023-40/

ISN 2023-19: Libwebp Vulnerability in Chromium and Other Software

Updated 28 September 2023 (fix versions, add CVE-2023-5129)

First published 14 September 2023

CVSS 3.1: 10.0 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Summary

A critical vulnerability has been found in Libwebp, used in the Chromium web browser and other software. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

A zero-day critical heap buffer overflow vulnerability has been found in the WebP library (Libwebp) used by Chromium, webkit2gtk, qt5 webkit, webengine and other software supporting the WebP image format. This vulnerability can be tracked with CVE-2023-4863 and CVE-2023-5129. Apple's Security Engineering and Architecture (SEAR) and The Citizen Lab are not publishing the details of this vulnerability as it has been seen exploited in-the-wild and they are giving time for people to update their browsers.

Update Instructions

- OS 12: Update to IGEL OS 12 base system version 12.2.1 (available on 17 October 2023) with an updated Libwebp.
- OS 11: Update to IGEL OS 11.09.100 (planned for 5 October 2023) with an updated Libwebp.

References

- CVE-2023-4863 - https://nvd.nist.gov/vuln/detail/CVE-2023-4863
- CVE-2023-5129 - https://nvd.nist.gov/vuln/detail/CVE-2023-5129
- Google's advisory - https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_11.html

ISN-2023-18: SnakeYAML Vulnerability

First published 30 August 2023

CVSS 3.1: 6.3 (Medium)

CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:L

Summary

A vulnerability has been found in the Java package snakeYAML, which is used to parse YAML files. This affects the following IGEL products:

- UMS
- ICG

Details

A deserialization vulnerability has been discovered in SnakeYAML. It can lead to Remote Code Execution (RCE). However, in IGEL UMS and ICG it cannot be called remotely. Also, an attack on the local YAML file is mitigated by the fact that this is only writeable by root or a Windows system service. This is why IGEL is downgrading the severity of this issue, rated by NVD as critical, to medium for UMS and ICG.

Update Instructions

- UMS: Update UMS to version 12.03.100 (scheduled for November 2023)
- ICG: Update ICG to version 12.03.100 (scheduled for November 2023)

References

- CVE-2022-1471: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1471
- NVD, CVE-2022-1471: https://nvd.nist.gov/vuln/detail/CVE-2022-1471

ISN 2023-17: AMD Inception CPU Vulnerability

First published 24 August 2023

CVSS 3.1: 5.6 (Medium)

CVSS: 3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N

Summary

A vulnerability named Inception has been discovered in some AMD CPUs. This affects the following IGEL Products

- IGEL OS 12 running on specific AMD CPUs
- IGEL OS 11 running on specific AMD CPUs

Details

It has been discovered that a local attacker could steal information from other users or VMs on the same system, or from the Linux kernel, on certain AMD processors. This vulnerability has been named Inception (CVE-2023-20569) and is rated as medium.

Such side channel threats mainly target environments with many VMs being hosted. This is not the case with IGEL OS. In addition, IGEL follows the general recommendation made by AMD in this case to prevent the execution of malware by keeping packages up to date and applying security policies through respective configuration.

Inception affects AMD's Zen 3 and Zen 4 architectures, including Ryzen and Athlon processors. The new CVE.org[15] site has a list at https://www.cve.org/CVERecord?id=CVE-2023-20569

AMD states that it is not aware of this vulnerability being exploited in the wild.

Update instructions

- OS 12: Install a BIOS version containing a microcode fix for this issue. Alternatively, wait for IGEL OS Base System version 12.3.0 (scheduled for December 2023) and update to that.
- OS 11: Install a BIOS version containing a microcode fix for this issue. Check whether you can utilize LVFS to deploy the update from UMS: *IGEL OS* > *IGEL OS Articles* > *BIOS Tools*

References

- ETH Zurich COMSEC, "Inception: how a simple XOR can cause a Microarchitectural Stack Overflow": https://comsec.ethz.ch/research/microarch/inception/
- AMD Return Address Security Bulletin (AMD-SB-7005): https://www.amd.com/en/resources/product-security/bulletin/amd-sb-7005.html
- CVE-2023-20569: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20569
- CVE-2023-20569 (new site): https://www.cve.org/CVERecord?id=CVE-2023-20569

15. http://CVE.org

ISN 2023-16: Intel Downfall CPU Vulnerability

First published 24 August 2023

CVSS 3.1: 6.5 (Medium)

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

Summary

A vulnerability nicknamed Downfall has been discovered in several Intel CPU lines. This affects the following IGEL Products

- IGEL OS 12 running on specific Intel CPUs
- IGEL OS 11 running on specific Intel CPUs

Details

Downfall (CVE-2022-40982) is a vulnerability in the memory optimization features in Intel processors. It can allow a local user to steal secrets from other users on the same system, and from the Linux Kernel. This is a threat mainly to environments where many VMs or many user accounts are hosted, but not so much IGEL OS, which only has one person using it.

This vulnerability is rated as medium. It affects Intel Core processors from the 6th Skylake to and including the 11th Tiger Lake generation.

The reporter of Downfall has published proof-of-concept exploit code.

Update Instructions

- OS 12: Update the IGEL OS Base System app to version 12.02.100 (available in September 2023)
- OS 11: Update to OS 11.09.100 (available in September 2023)

References

- Daniel Moghimi, “Downfall Attacks”: https://downfall.page/
- CVE-2022-40982: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40982

ISN 2023-15: ZenBleed Vulnerability

First published 28 July 2023

CVSS 3.1: 6.5 (Medium)

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

Summary

A vulnerability called ZenBleed has been discovered in the line of “Zen 2” CPUs from AMD. This affects the following IGEL Products

- IGEL OS 12 running on AMD CPUs
- IGEL OS 11 running on AMD CPUs

Details

ZenBleed (CVE-2023-20593) is a medium risk (6.5 CVSS score) vulnerability, which can allow local attackers with the ability to run arbitrary code within the local machine/VM to infer CPU register content from another process in the same instance scheduled on the same core. This could potentially leak sensitive information. Google’s Project Zero security team has confirmed that this vulnerability is reproducible on at least the following SKUs:

- AMD Ryzen Threadripper PRO 3945WX 12-Cores
- AMD Ryzen 7 PRO 4750GE with Radeon Graphics
- AMD Ryzen 7 5700U
- AMD EPYC 7B12

Update Instructions

- OS 12: Update the IGEL OS Base System app to version 12.02.100 (available in September 2023)
- OS 11: Update to OS 11.09.100 (available in September 2023)

References

- Vulnerability write-up by Tavis Ormandy (Google): https://lock.cmpxchg8b.com/zenbleed.html
- Google’s Project Zero Disclosure: https://github.com/google/security-research/tree/master/pocs/cpus/zenbleed

ISN 2023-14: IGEL OS OpenSSH Vulnerability

Updated 28 August 2023 (OS 11 fix version)

First published 26 July 2023

CVSS 3.1: 7.3 (High)

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Summary

A vulnerability has been discovered in OpenSSH, a remote shell used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

It has been found that specific libraries loaded via the PKCS#11 support in the ssh-agent command in OpenSSH could be abused by an attacker to achieve Remote Code Execution (RCE). This vulnerability (CVE-2023-38408) has been rated as high. The exploitation requires the presence of specific libraries on the victim system, and that the agent was forwarded to an attacker-controlled system. This is not done by default in IGEL OS, but customers could do this in a custom command or script.

Mitigation

- Customers usually do not utilize ssh-agent on IGEL OS.
- For those that use ssh-agent: According to the OpenSSH project, exploitation can be prevented by starting ssh-agent with an empty PKCS#11/FIDO allowlist (`ssh-agent -P ''`) or by configuring an allowlist that contains only specific provider libraries.

Update Instructions

- OS 12: Update the IGEL OS Base System app to version 12.02.100 (available in September 2023)
- OS 11: Update to the IGEL OS version 11.08.440.

References

- OpenSSH: Release Notes for OpenSSH 9.3p2: https://www.openssh.com/txt/release-9.3p2
- Qualys: CVE-2023-38408: Remote Code Execution in OpenSSH's forwarded ssh-agent: https://www.qualys.com/2023/07/19/cve-2023-38408/rce-openssh-forwarded-ssh-agent.txt

ISN 2023-13: IGEL OS Ghostscript Vulnerability

First published 24 July 2023

CVSS 3.1: 7.8 (High)

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

A vulnerability has been discovered in Ghostscript, a Postscript and PDF library used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

A security issue rated high has been found in Ghostscript (CVE-2023-36664). The software mishandles permission validation for pipe devices (with the %pipe% prefix or the | pipe character prefix). Abusing this, an attacker can achieve command execution with malformed documents that are processed by Ghostscript, e.g. Postscript, PDF and EPS files.

Mitigation

- General: Until this issue is fixed, print and view only documents from trustworthy sources.
- OS 11: If local printing from IGEL OS is not needed, you can remove Ghostscript from the system using a UMS profile:

1. In Setup, go to **System > Firmware Customization > Features**.
2. Disable the entries for **Printing (Internet Printing Protocol CUPS)**, **PrinterLogic**, and **NoMachine NX**.
3. Apply and Save the changes.
4. Reboot the devices.

Update Instructions

- OS 12: Update the IGEL OS Base System app to version 12.02.100 (available in September 2023)
- OS 11: Update to IGEL OS 11.09.100 (available in September 2023)

References

- CVE-2023-36664 at NVD: https://nvd.nist.gov/vuln/detail/CVE-2023-36664
- Kroll: Proof of Concept Developed for Ghostscript CVE-2023-36664 Code Execution Vulnerability: https://www.kroll.com/en/insights/publications/cyber/ghostscript-cve-2023-36664-remote-code-execution-vulnerability

ISN 2023-12: Citrix Secure Access Client

Updated 28. August 2023 (releases with fix added)

First published 17 July 2023

CVSS 3.1: 9.6 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Summary

A vulnerability was discovered in the Citrix Secure Access client, which affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

Citrix Secure Access client is the client software that allows access to corporate data and applications through Citrix ADC. Versions before 23.5.2 are vulnerable to remote code execution when a user opens an attacker-crafted link and accepts further prompts. This vulnerability is classified as critical (9.6 score) and is being tracked as CVE-2023-24492.

Update Instructions

- OS 12: Update the Citrix Gateway EPA client app to version 23.6.2 BUILD 2.0
- OS 11: Update to OS 11.09.100 (available in September 2023)

References

- Citrix's Security Bulletin: https://support.citrix.com/article/CTX564169/citrix-secure-access-client-for-ubuntu-security-bulletin-for-cve202324492

ISN 2023-11: “StackRot” in IGEL OS Kernel

First published 11 July 2023

CVSS 3.1: 7.8 (High)

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

Summary

A vulnerability has been discovered in the Linux kernel version used in IGEL OS. This affects the following IGEL products:

- IGEL OS 12

Details

A vulnerability found in the Linux kernel 6.1 memory management subsystem may allow a local attacker to execute arbitrary code and escalate their privileges to root. The issue (CVE-2023-3269), nicknamed StackRot, is graded as high. It is not easy to abuse it, but Ruihan Li, who reported the vulnerability, has announced he will release exploit code later in July.

Update Instructions

- OS 12: IGEL is preparing an OS 12 base system release with the kernel security fixes.

References

- [oss-security] Ruihan Li: StackRot (CVE-2023-3269): Linux kernel privilege escalation vulnerability: https://www.openwall.com/lists/oss-security/2023/07/05/1
- Ruihan Li: Github StackRot repository: https://github.com/lrh2000/StackRot

ISN 2023-10: Log4j 1.x in IBM i Access Client

First published 19 June 2023

CVSS 3.1: 8.1 (High)

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

A vulnerability has been discovered in the IBM i Access Client contained in IGEL OS. This affects the following IGEL products:

- IGEL OS 11

Details

IBM i Access Client is a terminal emulator for accessing IBM I series hosts. In version 1.1.8.6 and earlier, which have been shipped with IGEL OS 11, it contains the obsolete and unmaintained branch 1.x of the Log4j logging framework. This Log4j version could allow a remote attacker to execute arbitrary code on the system, which is a vulnerability rated as high (CVE-2021-4104). However, for this the attacker needs write access to the Log4j configuration – which is usually not the case on IGEL OS.

Mitigation

Many customers will not need the IBM i Access Client, so they can remove it completely in **Setup > System > Firmware Customization > Features**.

Update Instructions

- OS 11: IGEL is preparing an IGEL OS version with an updated IBM i Access Client.

References

- Security Bulletin: IBM i components are affected by CVE-2021-4104 (log4j version 1.x): https://www.ibm.com/support/pages/security-bulletin-ibm-i-components-are-affected-cve-2021-4104-log4j-version-1x

ISN 2023-09: RCE in CUPS Printing System

First published 07 June 2023

CVSS 3.1: 8.8 (High)

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Summary

A vulnerability has been discovered in CUPS Filters, which are shipped with IGEL OS. This affects the following IGEL products:

- IGEL OS 11
- IGEL OS 12

Details

A security vulnerability rated high has been found in CUPS Filters (CVE-2023-24805). When using the Backend Error Handler (beh) to create an accessible network printer, this security vulnerability can allow remote code execution (RCE).

Update Instructions

- OS 11: Update to IGEL OS version 11.08.330 or newer.
- OS 12: Update to IGEL OS base system version 12.01.120 (available 12 June 2023)

References

- CVE-2023-24805: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24805

ISN 2023-08: Chromium Critical Vulnerability

Updated 26 July 2023 (updated timelines)

First published 25 May 2023

CVSS 3.1: 9.8 (critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

A critical vulnerability has been found in the Chromium web browser used in IGEL OS.

This affects the following IGEL products:

- IGEL OS 11
- IGEL OS 12

Details

The Chrome project has announced that a use-after-free error has been discovered in the Navigation component of the Chromium browser before version 113 (CVE-2023-2721). This vulnerability potentially allows a remote attacker to exploit heap corruption via a crafted HTML page. It is rated critical.

Mitigation

- On IGEL OS 11, use Firefox as an alternative.

Update Instructions

- IGEL OS 11: Update to the upcoming IGEL OS 11.08.x August release.
- IGEL OS 12: Update the Chromium 114 app for OS 12 (available in the first week of August).

References

- Chrome Team – Stable Channel Update for Desktop: https://chromereleases.googleblog.com/2023/05/stable-channel-update-for-desktop_16.html

ISN 2023-07: Device Encryption Password Bug

First published 23 May 2023

CVSS 3.1: 2.3 (Low)

CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N

Summary

A bug in the IGEL OS Setup application prevents users from setting a (new) password for Device Encryption, and from disabling Device Encryption. This affects the following IGEL products:

- IGEL OS 11.08.290

Details

Due to a bug in the IGEL OS Setup application, users of IGEL OS 11.08.290

- cannot set a (new) password for Device Encryption
- cannot deactivate Device Encryption

The severity of this issue is low. Device Encryption settings and passwords that have been set before upgrading to IGEL OS 11.08.290 are not affected by this bug. They remain the same.

Mitigation

If you cannot update to IGEL OS 11.08.330 yet, you can apply the following mitigation:

1. Go to **Setup > System > Firmware Customization> Custom Commands**.
2. Enter the following command in the **Desktop initialization** field:
   `systemctl start igel-kml-daemon`
3. Reboot the system.

Update Instructions

- Update to IGEL OS version 11.08.330 (and set a Device Encryption password after the upgrade, if desired).

ISN 2023-06: UEFI Secure Boot Malware and IGEL OS

Updated 15 May 2023 (Windows Update does not block IGEL OS boot)

First published 12 May 2023

CVSS:3.1 6.7 / 6.2 (Medium)

CVSS:3.1 vector n/a

Summary

A fix for a UEFI Secure Boot issue may affect booting IGEL OS on some devices.

This affects the following IGEL products:

- IGEL OS 11
- IGEL OS 12
- IGEL UD Pocket

Details

In order to block UEFI Secure Boot malware such as the Black Lotus bootkit (CVE-2023-24932), Microsoft has published a security update that revokes a number of bootloaders from UEFI Secure Boot (KB5025885). Also, the UEFI Forum has updated their revocation list.

- IGEL has determined that the UEFI Forum revocation list of 9 May 2023 does not block the IGEL Shim bootloader. Customers that apply this revocation list will not have issues with booting IGEL OS.
- Applying Microsoft KB5025885 and its revocation command does not block the IGEL Shim bootloader either, testing at IGEL has shown.

References

- Microsoft, “Secure Boot Security Feature Bypass Vulnerability - CVE-2023-24932”: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24932
- Microsoft KB5025885: https://support.microsoft.com/en-us/topic/kb5025885-how-to-manage-the-windows-boot-manager-revocations-for-secure-boot-changes-associated-with-cve-2023-24932-41a975df-beb2-40c1-99a3-b3ff139f832d#timing5025885
- UEFI revocation list file (x64): https://uefi.org/revocationlistfile

ISN 2023-05: Chromium Local File Access

First published 3 April 2023

CVSS 3.1: 6.6 (Medium)

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L

Summary

The Chromium web browser in IGEL OS has been found to allow access to the local filesystem under certain circumstances. This affects the following IGEL products:

- IGEL OS 11

Details

A penetration test commissioned by IGEL has found that the Chromium browser on IGEL OS allows users to access the local filesystem even when it is forbidden in the profile settings – via downloads, bookmarks, and printing. This is fixed now, disabling downloads, bookmarks, and printing in Chromium when filesystem access is set to be blocked.

Update Instructions

- Update to IGEL OS 11.08.290

ISN 2023-04: IGEL OS Local Privilege Escalation

First published 3 April 2023

CVSS 3.1: 7.8 (High)

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Summary

The configuration mechanism in IGEL OS has been found to have two vulnerabilities rated high. This affects the following IGEL products:

- IGEL OS 11

Details

A penetration test commissioned by IGEL has found two instances of local privilege escalation in the IGEL OS configuration mechanism. A non-privileged user could employ these to become `root` on the local system. These issues are rated as high.

Update Instructions

- Update to IGEL OS 11.08.290

ISN 2023-03: Chromium Vulnerabilities

First published 22 March 2023

CVSS 3.1 High

CVSS:3.1 n/a

Summary

The Chromium browser in IGEL OS has been found to have several vulnerabilities rated high. This affects the following IGEL products:

- IGEL OS 11

Details

The Google Chrome project has reported numerous use-after-free vulnerabilities, among others in the Prompts component, which could allow a remote attacker to exploit heap corruption via a crafted HTML page (high, CVE-2023-0941). Further use-after-free weaknesses affect the Web Payments API, SwiftShader, Vulkan, Video and WebRTC.

Other issues include type confusions in the V8 JavaScript engine (high, CVE-2023-0696), Data Transfer (medium, CVE-2023-0702), and DevTools (medium, CVE-2023-0703).

Update Instructions

- Update to IGEL OS 11.08.290 (available in March 2023) which contains Chromium version 110.0.5481.177.

References

- Chrome Team – Stable Channel Update for Desktop: https://chromereleases.googleblog.com/2023/02/stable-channel-desktop-update_22.html
- Chrome Team – Stable Channel Update for Desktop: https://chromereleases.googleblog.com/2023/02/stable-channel-update-for-desktop.html
- Chrome Team – Stable Channel Update for Desktop: https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop_24.html

ISN 2023-02: Firefox ESR Vulnerabilities

First published 22 March 2023

CVSS 3.1 high

CVSS:3.1 n/a

Summary

Firefox ESR version 91.13.0, which has been in IGEL OS 11 since 11.08.200, has been found to have several vulnerabilities rated high.

- IGEL OS 11

Details

The vulnerabilities found include that the `Content-Security-Policy-Report-Only` header could allow an attacker to leak a child iframe's unredacted URI when interaction with that iframe triggers a redirect (high, CVE-2023-25728). A background script invoking `requestFullscreen` and then blocking the main thread could force the browser into fullscreen mode indefinitely, resulting in potential user confusion or spoofing attacks (high, CVE-2023-25730).

In addition, there are arbitrary file reads from GTK drag and drop (high, CVE-2023-23598) and from a compromised content process that partially escaped the sandbox (high, CVE-2022-46872). A same-origin policy violation could leak cross-origin URLs (high, CVE-2022-42927).

Firefox ESR version 91.13.0 is also affected by memory safety bugs that can lead to application crashes or to the execution of arbitrary code.

Update Instructions

- Update to IGEL OS 11.08.290 which has Firefox ESR version 102.8.0 (available in March 2023).

References

- Mozilla Foundation Security Advisory 2023-06: https://www.mozilla.org/en-US/security/advisories/mfsa2023-06/
- Mozilla Foundation Security Advisory 2023-02: https://www.mozilla.org/en-US/security/advisories/mfsa2023-02/
- Mozilla Foundation Security Advisory 2022-52: https://www.mozilla.org/en-US/security/advisories/mfsa2022-52/
- Mozilla Foundation Security Advisory 2022-48: https://www.mozilla.org/en-US/security/advisories/mfsa2022-48/
- Mozilla Foundation Security Advisory 2022-45: https://www.mozilla.org/en-US/security/advisories/mfsa2022-45/

- Mozilla Foundation Security Advisory 2022-41: https://www.mozilla.org/en-US/security/advisories/mfsa2022-41/

ISN 2023-01: Citrix Workspace App Vulnerability

Updated 28th February 2023 (Citrix advises updating to CWA 2302 as the only fix)

First published 20 February 2023

CVSS 3.1 High

CVSS:3.1 n/a

Summary

A vulnerability has been found in the Citrix Workspace App (CWA) for Linux in versions before 2302. The following IGEL products are affected:

- IGEL OS 11

Details

Citrix advises that there is a vulnerability in Citrix Workspace app for Linux that, if exploited, may result in a malicious local user being able to gain access to the Citrix Virtual Apps and Desktops session of another user who is using the same computer from which the ICA session is launched. This issue affects all supported versions of Citrix Workspace app for Linux before 2302.

Update Instructions

- Update to IGEL OS version 11.08.255, which contains CWA 2302, and use this version. It is available to IGEL customers as a private build from IGEL Customer Engineering.

References

- Citrix Workspace app for Linux Security Bulletin for CVE-2023-24486: https://support.citrix.com/article/CTX477618/citrix-workspace-app-for-linux-security-bulletin-for-cve202324486

ISN 2022-21: Chromium Vulnerability

First published 15 September 2022

CVSS 3.1 High

CVSS:3.1 n/a

Summary

A vulnerability has been found in the Chromium web browser used in IGEL OS. This affects the following IGEL products:

- IGEL OS 11

Details

A vulnerability has been found in the Mojo library collection used in Chromium (CVE-2022-3075). It is rated high and is caused by insufficient data validation. Google is aware of reports that an exploit for this issue exists in the wild.

Update Instructions

- IGEL OS 11: Update to IGEL OS version 11.08.200 (release planned for mid-October)

References

- Chrome Team – Stable Channel Update for Desktop: https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop.html

ISN 2022-20: Firefox ESR Vulnerabilities

First published 15 September 2022

CVSS 3.1 High

CVSS:3.1 n/a

Summary

Multiple vulnerabilities have been found in the Firefox ESR web browser used in IGEL OS. This affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

Three vulnerabilities rated high have been found in Firefox ESR. An attacker could abuse XSLT error handling to associate attacker-controlled content with another origin which was displayed in the address bar. This could have been used to fool the user into submitting data intended for the spoofed origin (CVE-2022-38472). Another vulnerability affects a cross-origin iframe referencing an XSLT document – it would inherit the parent domain's permissions such as microphone or camera access (CVE-2022-38473). The third issue concerns memory safety bugs that could be exploited to run arbitrary code (CVE-2022-38478).

Update Instructions

- IGEL OS 11: Update to IGEL OS version 11.08.200 (release planned for mid-October)
- IGEL OS 10: Upgrade to the fixed IGEL OS 11 version

References

- Mozilla Foundation Security Advisory 2022-35: https://www.mozilla.org/en-US/security/advisories/mfsa2022-35/

ISN 2022-19: Log4j 1.x Remainder in UMS

Updated 17 October 2022 (UMS version 6.10.130 available)

First published 12 September 2022

CVSS 3.1: 3.4 (Low)

CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:L

Summary

Universal Management Suite (UMS) has been found to still contain an obsolete and vulnerable Log4j version.
Affected products:

- UMS on Windows with High Availability (HA) option installed
- UMS on Linux, default installation

Details

Although IGEL has replaced most of Log4j in UMS with a different logging solution, UMS up to version 6.10.120 still contains an instance of Log4j version 1.x. It is located at `messageservice/lib/optional/log4j-1.2.14.jar` in the UMS installation directory.

This version is unmaintained, and the application's confidentiality and availability could have a low impact due to the vulnerabilities associated with version 1.x.

UMS contains further files with log4j in their filenames, such as `log4j-api-2.17.1.jar`. These are no indicator of vulnerable Log4j versions being present. Rather, they are API bridges used by IGEL to replace Log4j with a different logging solution. They pose no risk.

Do not delete files from IGEL UMS installations. This will break the application.

Update Instructions

- Update to UMS version 6.10.130

References

- Apache Software Foundation Blog, "Apache™ Logging Services™ Project announces Log4j™ 1 end-of-life; recommends upgrade to Log4j 2": https://news.apache.org/foundation/entry/apache_logging_services_project_announces

ISN 2022-18: Linux Kernel Vulnerability

First published 7 September 2022

CVSS 3.1 7.8 (High)

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Summary

A vulnerability has been found in the Linux kernel used by IGEL OS. This affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

A use-after-free vulnerability has been discovered in the Netfilter subsystem in the Linux kernel (CVE-2022-32250, formerly also known as CVE-2022-1966). It is rated high and allows a local non-privileged user to escalate their privileges to root.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.08.100 or newer.
- IGEL OS 10: Upgrade to the fixed IGEL OS 11 version.

References

- CVE-2022-32250: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32250

ISN 2022-17: Chromium WebRTC Vulnerability

Updated 30 August 2022 (IGEL OS 11.08.100 available)

First published 22 July 2022

CVSS 3.1 High

CVSS: n/a

Summary

Multiple vulnerabilities have been found in the Chromium web browser. This affects the following IGEL products:

- IGEL OS 11

Details

Google has reported a heap buffer overflow in the WebRTC component (CVE-2022-2294), which is used for multimedia and video conferencing. Google has rated this as high and states that an exploit for this issue exists in the wild. The other vulnerability rated high is a type confusion in the V8 JavaScript engine (CVE-2022-2295).

Update Instructions

- IGEL OS 11: Update to IGEL OS version 11.08.100 or newer.

References

- Chrome Team – Stable Channel Update for Desktop: https://chromereleases.googleblog.com/2022/07/stable-channel-update-for-desktop.html

ISN 2022-16: Firefox Vulnerabilities

Updated 1st July 2022 (IGEL OS 11.07.170 available)

First published 24th June 2022

CVSS 3.1 Critical

CVSS:3.1 n/a

Summary

Critical vulnerabilities have been found in the Firefox ESR browser. This affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

It has been discovered that an attacker who could corrupt the methods of an Array object in JavaScript via prototype pollution could execute attacker-controlled JavaScript code in a privileged context (CVE-2022-1802). In addition, an attacker could have sent a message to the parent process where the contents were used to double-index into a JavaScript object, leading to prototype pollution and ultimately attacker-controlled JavaScript executing in the privileged parent process (CVE-2022-1529). Both issues are considered critical.
Update instructions

- IGEL OS 11: Update to IGEL OS 11.07.170, which contains Firefox ESR 91.9.1.
- IGEL OS 10: Upgrade to IGEL OS 11.07.170.

References

Mozilla Foundation Security Advisory 2022-19: https://www.mozilla.org/en-US/security/advisories/mfsa2022-19/

ISN 2022-15: Chromium Browser Vulnerabilities

Updated 1st July 2022 (IGEL OS 11.07.170 available)

First published 20th June 2022

CVSS 3.1 Critical

CVSS:3.1 n/a

Summary

The Chromium project has reported multiple vulnerabilities in its web browser. These affect the following IGEL products:

- IGEL OS 11

Details

It has been discovered that the Indexed DB component in Chromium contains a use-after-free error. The project rates this vulnerability as critical (CVE-2022-1853). Eight further memory management issues, mostly use-after-free, exist in several other Chromium components. These have been rated as high (CVE-2022-1854, CVE-2022-1855, CVE-2022-1856, CVE-2022-1857, CVE-2022-1858, CVE-2022-1859, CVE-2022-1860, CVE-2022-1861).

Besides that, several vulnerabilities rated as medium and low exist in Chromium. They are listed in the referenced update from the Chrome Team.

Update instructions

- IGEL OS 11: Update to IGEL OS 11.07.170, which contains Chrome 102.

References

- Chrome Team – Stable Channel Update for Desktop: https://chromereleases.googleblog.com/2022/05/stable-channel-update-for-desktop_24.html
- CVE-2022-1853: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1853

ISN 2022-14: Chromium Browser Vulnerabilities

First published 3rd June 2022

CVSS 3.1 High

CVSS:3.1 n/a

Summary

The Chromium project has reported multiple vulnerabilities in its web browser. These affect the following IGEL products:

- IGEL OS 11

Details

An inappropriate implementation in Web Contents has been found in Chromium and has been rated as high (CVE-2022-1637). In addition, there are 6 issues of use-after-free which are rated high (CVE-2022-1633, CVE-2022-1634, CVE-2022-1635, CVE-2022-1636, CVE-2022-1639, CVE-2022-1640) and one such issue rated medium (CVE-2022-1641). Besides that, a heap buffer overflow has been found in V8 internationalization and rated high (CVE-2022-1638).

Update Instructions

- IGEL OS 11: Update to IGEL OS version 11.07.140, which contains Chromium version 101 or newer.

References

- Chrome Team – Stable Channel Update for Desktop: https://chromereleases.googleblog.com/2022/05/stable-channel-update-for-desktop_10.html
- CVE-2022-1637: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1637
- CVE-2022-1638: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1638

ISN 2022-13: UMS Vulnerabilities

Updated 8th June (clarification of update availability)

First published 25th May 2022

CVSS 3.1 Base Score: 8.6 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

Summary

Several security issues have been found in IGEL Universal Management Suite (UMS). This affects the following IGEL products:

- UMS 6.x

Details

It has been discovered that IGEL UMS on Windows stores superuser/database credentials in the `HKEY_LOCAL_MACHINE` registry, which allows a low-privileged attacker with Operating System (OS) access to read the encrypted `dbpassword` value (CVE-2022-25804).

Another vulnerability is a hardcoded DES key which allows an attacker with access to an encrypted `dbpassword` value to decrypt the password and gain superuser/database access to IGEL UMS and its database (CVE-2022-25806).

Another hardcoded DES key allows an attacker with access to encrypted LDAP bind credentials to decrypt the password and obtain access to plaintext LDAP bind credentials (CVE-2022-25807).

Finally, UMS may expose Lightweight Directory Access Protocol (LDAP) bind credentials in plaintext form, which allows a remote, authenticated attacker to obtain access to those credentials (CVE-2022-25805).

These issues were found by Nick Nam of Atredis Partners.

Mitigations

- CVE-2022-25804 can be mitigated by using a dedicated host for the UMS server and restricting access to it to the UMS administrator only. Using a dedicated host per service is a general IT Best Practice.
- CVE-2022-25806 and CVE-2022-25807 can be mitigated by restricting access to the UMS database and its backups.
- CVE-2022-25805 can be mitigated by using LDAPS (with TLS) only, which is configurable in UMS.

Update Instructions

- UMS 6.x: A UMS release with fixes is in preparation. When it is available, this ISN will be updated.

References

- Atredis Partners, Multiple Vulnerabilities in IGEL Universal Management Suite (UMS) v6.07.100: https://github.com/atredispartners/advisories/blob/master/ATREDIS-2022-0002.md
- CVE-2022-25804: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25804
- CVE-2022-25806: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25806
- CVE-2022-25807: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25807
- CVE-2022-25805: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25805

ISN 2022-12: Teradici PCoIP Library Vulnerabilities

Updated 2nd June 2022 (IGEL OS 11.07.140 available)

First published 9th May 2022

CVSS 3.1 Base Score: High

CVSS:3.1 n/a

Summary

Multiple vulnerabilities have been found in libraries bundled with the Teradici PCoIP client for Linux. This affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

The Libexpat version bundled with the Teradici PCoIP client for Linux is affected by three critical issues (CVE-2022-22822, CVE-2022-22823, and CVE-2022-22824) and five issues rated high. Overall, the vendor HP rates the severity in the product context as high.

The OpenSSL version bundled with the Teradici PCoIP client for Linux has one issue rated high (CVE-2022-0778) and one rated medium (CVE-2021-4160). Overall, the vendor HP rates the severity in the product context as high.

The full list of CVEs can be found in the HP advisories given in the References section.

Update Instructions

- IGEL OS 11: Update to IGEL OS version 11.07.140 or newer.
- IGEL OS 10: Upgrade to IGEL OS version 11.07.140 or newer.

References

- HP, „Expat Library update for Teradici PCoIP Software and Firmware“: https://support.hp.com/us-en/document/ish_6052753-6052783-16/hpsbhf03750
- HP, “OpenSSL update for Teradici PCoIP”: https://support.hp.com/us-en/document/ish_6052720-6052798-16/hpsbhf03784

ISN 2022-11: VMware Horizon Privilege Escalation

Updated 2nd June 2022 (IGEL OS 11.07.140 available)

First published 26th April 2022

CVSS 3.1 Base Score: 7.3 (High)

CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

Summary

Two vulnerabilities have been found in VMware Horizon Client for Linux. This affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

The first issue (CVE-2022-22962) allows a local non-privileged user to change the default shared folder location due to a vulnerable symbolic link. This can result in linking to a file owned by root.
The second issue (CVE-2022-22964) lets a local non-privileged user escalate their privileges to root due to a vulnerable configuration file.

Update Instructions

- IGEL OS 11: Update to IGEL OS version 11.07.140 or newer.
- IGEL OS 10: Upgrade to IGEL OS version 11.07.140 or newer.

Mitigation

This issue can be mitigated by not giving users access to a terminal/virtual console on IGEL OS, which they could use to configure and run the exploit code:

Remove an existing local terminal session:

1. In IGEL Setup, go to **Accessories > Terminals**.
2. Select a local terminal session you want to delete.
3. Click the trash icon to remove the selected session.
4. When prompted, confirm that you want to delete the session.
5. Click **Apply**.

Or password-protect the local terminal with the Administrator password:

1. Find the local terminal session under **Accessories > Terminals**.

2. Follow the instructions under *IGEL OS PUBLIC* > *Versions of IGEL OS* > *(11.09-en)* IGEL OS > *(11.09-en)* IGEL OS Articles > *(11.09-en)* Security > *(11.09-en)* Security IGEL OS Endpoints > *(11.09-en) Setting Passwords* > *(11.09-en) Password-Protecting Sessions and Accessories*.

Disable virtual console access:

1. In IGEL Setup, go to **User Interface > Display > Access Control**.
2. Activate **Disable console switching** (Default: Console switching enabled)
3. Click **Apply**.

References

VMSA-2022-0012: https://www.vmware.com/security/advisories/VMSA-2022-0012.html

ISN 2022-10: Firefox Vulnerabilities

Updated 2nd June 2022 (IGEL OS 11.07.140 available)

First published 19th April 2022

CVSS 3.1 Base Score: 7.5 (High)

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

Multiple vulnerabilities have been found in the Firefox ESR Browser. This affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

The Firefox ESR Browser used in IGEL OS is affected by seven security issues rated as high. This includes a browser window spoof using fullscreen mode (CVE-2022-26383) and a bypass for the JavaScript sandbox in iframes (CVE-2022-26384). Another vulnerability affects the verification of add-on signatures: When installing an add-on, Firefox verifies the signature before prompting the user; but while the user is confirming the prompt, the underlying add-on file can be modified, and Firefox would not notice (CVE-2022-26387). The other defects concern memory safety. A full list of CVEs is available in the Mozilla advisories listed in "References".

Mitigation

CVE-2022-26387 can be mitigated by not installing new add-ons until a fixed version of Firefox ESR has been installed.

Update Instructions

- IGEL OS 11: Update to IGEL OS version 11.07.140 or newer.
- IGEL OS 10: Upgrade to IGEL OS version 11.07.140 or newer.

References

- Mozilla Foundation Security Advisory 2022-14: https://www.mozilla.org/en-US/security/advisories/mfsa2022-14/
- Mozilla Foundation Security Advisory 2022-11: https://www.mozilla.org/en-US/security/advisories/mfsa2022-11/

ISN 2022-09: Zlib Vulnerability

Updated 29th April 2022 (IGEL OS 11.07.110 available)

First published 8th April 2022

CVSS 3.1 Base Score: 8.2 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H

Summary

A vulnerability has been found in the Zlib compression library. This affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

When compressing specially crafted input, Zlib can run into an error that causes memory corruption, could crash applications, and could potentially lead to code execution. This issue has been registered as CVE-2018-25032 and is rated as high.

Update instructions

- IGEL OS 11: Update to IGEL OS 11.07.110 or newer.
- IGEL OS 10: Upgrade to IGEL OS 11.07.110 or newer.

References

CVE-2018-25032: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-25032

ISN 2022-08: Chromium JavaScript Vulnerability

Updated 29th April 2022 (IGEL OS 11.07.110 available)

First published 28th March 2022

Base Score: High

CVSS:3.1 vector not available yet

Summary

A vulnerability has been found in the Chromium browser. This affects the following IGEL products:

- IGEL OS 11

Details

It has been discovered that Chromium's JavaScript engine contains a vulnerability (CVE-2022-1096) that can be exploited when the user visits a web page that is under the control of an attacker. Google rates this issue as high and reports that it is being actively exploited in the wild.

Mitigation

- Use the Firefox Browser in IGEL OS 11.07.100 as an alternative, which is secured by AppArmor.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.07.110 or newer.

References

- Chrome Team – Stable Channel Update for Desktop: https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop_25.html
- CVE-2022-1096: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1096

ISN 2022-07: Chromium Browser Vulnerabilities

First published 22nd March 2022

CVSS 3.1 Base Score: 9.8 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

The Chromium project has reported multiple vulnerabilities in its web browser. These affect the following IGEL products:

- IGEL OS 11

Details

It has been discovered that the renderer in Chromium contains a use-after-free vulnerability which is rated critical (CVE-2022-0971). Eight further memory corruption issues have been reported which are rated high (CVE-2022-0972, CVE-2022-0973, CVE-2022-0974, CVE-2022-0975, CVE-2022-0976, CVE-2022-0977, CVE-2022-0978, CVE-2022-0979), and one medium (CVE-2022-0980).

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.07.100 (to be released on March 29th)

References

- Chrome Team – Stable Channel Update for Desktop: https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop_15.html
- CVE-2022-0971: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0971

ISN 2022-06: OpenSSL Denial of Service

First published 21st March 2022

CVSS 3.1 Base Score: 7.5 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Summary

A vulnerability has been found in the OpenSSL cryptography library. This affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

It has been discovered that OpenSSL can run into an infinite loop when parsing a TLS certificate or key that has invalid explicit elliptic curve parameters (CVE-2022-0778). An attacker could use a crafted and self-signed certificate to cause a denial of service in OpenSSL and consequently in applications that use OpenSSL.

Mitigation

The attack relies on a TLS server certificate crafted by an attacker. Until the security fix is available, only connect to servers under control of your own organization or a trusted party.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.07.100 (to be released on March 29th)
- IGEL OS 10: Upgrade to IGEL OS 11.07.100 (to be released on March 29th)

References

- OpenSSL Security Advisory - Infinite loop in BN_mod_sqrt() reachable when parsing certificates (CVE-2022-0778): https://www.openssl.org/news/secadv/20220315.txt
- CVE-2022-0778: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0778

ISN 2022-05: Netfilter Escalation of Privilege

First published 14th March 2022

CVSS 3.1 Base Score: 7.8 (High)

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Summary

A vulnerability has been found in the Netfilter component in the Linux kernel. This affects the following IGEL products:

- IGEL OS 11

Details

An out-of-bounds (OOB) memory access flaw has been found in the Netfilter code of the Linux kernel (CVE-2022-25636). This can enable an unprivileged local user to escalate their privileges or crash the system.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.07.100 (to be released on March 29th)

Mitigation

This issue can be mitigated by not giving users access to a terminal/virtual console on IGEL OS, which they could use to configure and run the exploit code:

Remove an existing local terminal session:

1. In IGEL Setup, go to **Accessories > Terminals**.
2. Select a local terminal session you want to delete.
3. Click the trash icon to remove the selected session.
4. When prompted, confirm that you want to delete the session.
5. Click **Apply**.

Or password-protect the local terminal with the Administrator password:

1. Find the local terminal session under **Accessories > Terminals**.
2. Follow the instructions under *IGEL OS PUBLIC > Versions of IGEL OS > (11.09-en)* IGEL OS *> (11.09-en)* IGEL OS Articles *> (11.09-en)* Security *> (11.09-en)* Security IGEL OS Endpoints *> (11.09-en) Setting Passwords > (11.09-en) Password-Protecting Sessions and Accessories*.

Disable virtual console access:

1. In IGEL Setup, go to **User Interface > Display > Access Control**.
2. Activate **Disable console switching** (Default: Console switching enabled)
3. Click **Apply**.

References

- CVE-2022-25636: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25636

ISN 2022-04: Dirty Pipe Escalation of Privilege

First published 10th March 2022

CVSS 3.1 Base Score: 8.4 (High)

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

A vulnerability in the Linux kernel, nicknamed "Dirty Pipe", affects the following IGEL products:

- IGEL OS 11

Details

Dirty Pipe (CVE-2022-0847) is a vulnerability that has been found in Linux kernels since version 5.8. It enables an unprivileged local user to write to files that should be writeable for root only. By adding commands to root's cron jobs or adding lines to the `/etc/passwd` file, for example, the attacker could escalate privilege and become root on the system.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.07.100.

Mitigation

This issue can be mitigated by not giving users access to a terminal/virtual console on IGEL OS, which they could use to configure and run the exploit code:

Remove an existing local terminal session:

1. In IGEL Setup, go to **Accessories > Terminals**.
2. Select a local terminal session you want to delete.
3. Click the trash icon to remove the selected session.
4. When prompted, confirm that you want to delete the session.
5. Click **Apply**.

Or password-protect the local terminal with the Administrator password:

1. Find the local terminal session under **Accessories > Terminals**.
2. Follow the instructions under *IGEL OS > Versions of IGEL OS > (11.09-en) IGEL OS > (11.09-en) IGEL OS Articles > (11.09-en) Security > (11.09-en) Security IGEL OS Endpoints > (11.09-en) Setting Passwords > (11.09-en) Password-Protecting Sessions and Accessories*.

Disable virtual console access:

1. In IGEL Setup, go to **User Interface > Display > Access Control**.
2. Activate **Disable console switching** (Default: Console switching enabled)
3. Click **Apply**.

References

- CVE-2022-0847: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0847
- Max Kellerman, “The Dirty Pipe Vulnerability”: https://dirtypipe.cm4all.com

ISN 2022-03: Glibc Denial of Service in IGEL OS

First published 9th March 2022

CVSS 3.1 Base Score: 8.1 (High)

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

Multiple vulnerabilities have been found in the GNU C Library (glibc). This affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

Security issues have been discovered in Glibc features such as iconv (CVE-2016-10228, CVE-2019-25013, CVE-2020-27618, CVE-2020-29562, CVE-2021-3326), nscd (CVE-2021-27645) and sunrpc (CVE-2022-23218, CVE-2022-23219). A remote attacker could use these to cause the GNU C Library to hang or crash, resulting in a denial of service. Additionally, the features wordexp (CVE-2021-35942) and realpath (CVE-2021-3998) could be made to disclose information. The vulnerability in getcwd (CVE-2021-3999) could possibly be used to execute arbitrary code.

Update Instructions

- IGEL OS 11: Update to version 11.07.100 (to be released on 29th March 2022) or newer
- IGEL OS 10: Upgrade to IGEL OS 11.07.100 (to be released on 29th March 2022) or newer

Mitigation

- The issues CVE-2022-23218 and CVE-2022-23219 in sunrpc can be mitigated by mounting NFS shares from trusted NFS servers only.

References

- USN-5310-1: GNU C Library vulnerabilities: https://ubuntu.com/security/notices/USN-5310-1
- CVE-2016-10228: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10228
- CVE-2019-25013: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-25013
- CVE-2020-27618: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27618
- CVE-2020-29562: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29562
- CVE-2021-3326: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3326
- CVE-2021-27645: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27645
- CVE-2022-23218: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23218
- CVE-2022-23219: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23219
- CVE-2021-35942: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35942

- CVE-2021-3998: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3998
- CVE-2021-3999: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3999

ISN 2022-02: UEFI Vulnerabilities in UD Devices

Updated 21 July 2022 (IGEL OS 11.08.100 will bring remediation)

Updated 24 February 2022 (updated "Update Instructions")

First published 10 February 2022

CVSS 3.1 Base Score: 8.2 (High)

CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Summary

Multiple vulnerabilities have been found in UEFI firmware. Several of these also affect the Insyde H2O UEFI firmware used on some IGEL devices. Insyde have not completed their investigation fully, but at present the following IGEL devices are affected:

- UD3-LX 60 (M350C)
- UD7-LX 20 (H860C)

Details

The Insyde H2O UEFI firmware contains multiple memory management vulnerabilities in System Management Mode (SMM). A local attacker with administrator privileges could use these vulnerabilities to elevate their privileges above the installed operating system in order to execute code in SMM mode. This could enable the attacker to invalidate hardware security features such as UEFI Secure Boot, install persistent malware, or create backdoors for information disclosure.

Update Instructions

- IGEL OS 11.08.100 (planned to be released in mid-August) will provide a method of deploying the UEFI updates from UMS via network.

Mitigation

- Set a UEFI password, see *IGEL OS > Versions of IGEL OS > (11.09.310-en) IGEL OS > (11.09.310-en) IGEL OS Articles > (11.09.310-en) Security > (11.09.310-en) Security IGEL OS Endpoints > (11.09.310-en) Setting Passwords > (11.09.310-en) Setting a UEFI Password*.
- Activate UEFI Secure Boot (default on IGEL UD devices), see UEFI Secure Boot Enabling Guides (see page 222).
- Do not allow booting from USB storage media, see *IGEL OS > Versions of IGEL OS > (11.09.310-en) IGEL OS > (11.09.310-en) IGEL OS Articles > (11.09.310-en) Security > (11.09.310-en) Security IGEL OS Endpoints > (11.09.310-en) Minimizing the Attack Surface > (11.09.310-en) Disabling USB Boot*.

This issue can be mitigated further by not giving users access to a terminal/virtual console on IGEL OS, which they could use to configure and run exploit code:

Remove an existing local terminal session

1. In IGEL Setup, go to **Accessories > Terminals**.
2. Select a local terminal session you want to delete.
3. Click the trash icon to remove the selected session.
4. When prompted, confirm that you want to delete the session.
5. Click **Apply**.

Or password-protect the local terminal with the Administrator password

1. Find the local terminal session under **Accessories > Terminals**.
2. Follow the instructions under *IGEL OS > Versions of IGEL OS > (11.09.310-en) IGEL OS > (11.09.310-en) IGEL OS Articles > (11.09.310-en) Security > (11.09.310-en) Security IGEL OS Endpoints > (11.09.310-en) Setting Passwords > (11.09.310-en) Password-Protecting Sessions and Accessories*.

Disable virtual console access

1. In IGEL Setup, go to **User Interface > Display > Access Control**.
2. Activate **Disable console switching**. (Default: Console switching enabled)
3. Click **Apply**.

References

- Insyde Software Security Advisory, listing all related CVEs: https://www.insyde.com/security-pledge
- CERT Coordination Center, “InsydeH2O UEFI software impacted by multiple vulnerabilities in SMM”: https://kb.cert.org/vuls/id/796611

ISN 2022-01: Polkit Escalation of Privilege

Updated 7 February 2022 (IGEL OS 11.06.250 released)

First published 27 January 2022

CVSS 3.1 Base Score: 7.8 (High)

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Summary

A vulnerability has been found in Polkit, a software component that allows users to execute programs as another user - often as root, - after providing a password. This affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

Polkit (formerly known as PolicyKit) has a privilege escalation vulnerability that allows an attacker with regular user privileges to become root without a password. This vulnerability (CVE-2021-4034), nicknamed PwnKit, has been rated as high. A working proof-of-concept exploit is available on the Internet.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.06.250.
- IGEL OS 10: Upgrade to IGEL OS 11.06.250.

Mitigation

This issue can be mitigated by not giving users access to a terminal/virtual console on IGEL OS, which they could use to configure and run the exploit code:

Remove an existing local terminal session:

1. In IGEL Setup, go to **Accessories > Terminals**.
2. Select a local terminal session you want to delete.
3. Click the trash icon to remove the selected session.
4. When prompted, confirm that you want to delete the session.
5. Click **Apply**.

Or password-protect the local terminal with the Administrator password:

1. Find the local terminal session under **Accessories > Terminals**.

2. Follow the instructions under *IGEL OS > Versions of IGEL OS > (11.09.310-en) IGEL OS > (11.09.310-en) IGEL OS Articles > (11.09.310-en) Security > (11.09.310-en) Security IGEL OS Endpoints > (11.09.310-en) Setting Passwords > (11.09.310-en) Password-Protecting Sessions and Accessories*..

Disable virtual console access:

1. In IGEL Setup, go to **User Interface > Display > Access Control**.
2. Activate **Disable console switching** (Default: Console switching enabled)
3. Click **Apply**.

References

- CVE-2021-4034: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4034
- Qualys Security Advisory: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt

ISN 2021-11: UMS Log4j Vulnerability

Updated 14 February 2022 (corrected statements on CVE-2021-4104)

Updated 12 January 2022 (added CVE-2921-44832 and note on ICG)

Updated 22 December 2021 (updated CVEs, removed mitigations, added fixed UMS version)

Updated 16 December 2021 (added affected versions, corrected mitigation for Elasticsearch on Windows)

First published 13 December 2021

CVSS 3.1 Base Score:10.0 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Summary

A critical vulnerability, also known as Log4shell, has been found in the Log4j logging library. This affects the following IGEL products (other IGEL products are not affected):

- IGEL Universal Management Suite (UMS), all versions since 5.09.100

Details

The versions 2.0-beta9 up to 2.14.1 of the Log4j library are vulnerable to Remote Command Execution (CVE-2021-44228). This means that a remote attacker can execute commands over the network on software that contains the vulnerable Log4j versions. IGEL UMS and the Elasticsearch engine in the IGEL UMS Web App are affected.

Exploit code is already available, and the issue is being actively exploited on the Internet. Therefore, IGEL strongly recommends updating all UMS installations.

In a typical UMS installation, this issue is mitigated by the fact that UMS is not reachable from the Internet.

In early attempts to fix CVE-2021-44228, further vulnerabilities have been found and assigned the identifiers CVE-2021-45046 and CVE-2021-45105. These affect the Context Lookup feature in Log4j, which UMS does not use, therefore UMS is not affected by these. Also, UMS is not affected by CVE-2021-44832, as it does not use the vulnerable features in Log4j version 2.17.

In addition, a vulnerability has been found in Log4j version 1.2.17 (CVE-2021-4104), which does not affect UMS, as the CVE applies only “when the attacker has write access to the Log4j configuration”, which is not the case in UMS.

> **Note on ICG**
> IGEL Cloud Gateway 2.04.100 contains Log4j version 1.2.17, but it is not affected by CVE-2021-4104, as it applies only “when the attacker has write access to the Log4j configuration”, which is not the case in ICG.

Update Instructions

- Update to UMS 6.09.120, which contains Log4j version 2.17

Mitigation

Older mitigation measures have been discredited. The safest course of action is to update to the fixed version.

References

- Log4j - Apache Log4j Security Vulnerabilities: https://logging.apache.org/log4j/2.x/security.html
- CVE-2021-44228: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228
- CVE-2021-45046: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046
- CVE-2021-45045: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45045
- CVE-2021-4104: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4104
- CVE-2021-44832: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44832

ISN 2021-10: Chromium vulnerabilities

First published 30 November 2021

CVSS 3.1 Base Score: 9.8 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

Many vulnerabilities have been found in the Chromium web browser, some rated as critical. These affect the following IGEL products:

- IGEL OS 11

Details

The Chromium project has reported many vulnerabilities in its browser, including issues graded as critical and high.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.06.210.

References

CVE-2021-37973, CVE-2021-37972, CVE-2021-37971, CVE-2021-37970, CVE-2021-37969, CVE-2021-37968, CVE-2021-37967, CVE-2021-37966, CVE-2021-37965, CVE-2021-37964, CVE-2021-37963, CVE-2021-37962, CVE-2021-37961, CVE-2021-37960, CVE-2021-37959, CVE-2021-37958, CVE-2021-37957, CVE-2021-37956, CVE-2021-30633, CVE-2021-30632, CVE-2021-30631, CVE-2021-30630, CVE-2021-30629, CVE-2021-30628, CVE-2021-30627, CVE-2021-30626, CVE-2021-30625, CVE-2021-30624, CVE-2021-30623, CVE-2021-30622, CVE-2021-30621, CVE-2021-30620, CVE-2021-30619, CVE-2021-30618, CVE-2021-30617, CVE-2021-30616, CVE-2021-30615, CVE-2021-30614, CVE-2021-30613, CVE-2021-30612, CVE-2021-30611, CVE-2021-30610, CVE-2021-30609, CVE-2021-30608, CVE-2021-30607, CVE-2021-30606, CVE-2021-30604, CVE-2021-30603, CVE-2021-30602, CVE-2021-30601, CVE-2021-30600, CVE-2021-30599, CVE-2021-30598, CVE-2021-30597, CVE-2021-30596, CVE-2021-30594, CVE-2021-30593, CVE-2021-30592, CVE-2021-30591, CVE-2021-30590, CVE-2021-30589, CVE-2021-30588, CVE-2021-30587, CVE-2021-30586, CVE-2021-30585, CVE-2021-30584, CVE-2021-30583, CVE-2021-30582, CVE-2021-30581, CVE-2021-30580, CVE-2021-30579, CVE-2021-30578, CVE-2021-30577, CVE-2021-30576, CVE-2021-30575, CVE-2021-30574, CVE-2021-30573, CVE-2021-30572, CVE-2021-30571, CVE-2021-30569, CVE-2021-30568, CVE-2021-30567, CVE-2021-30566, CVE-2021-30565, CVE-2021-37976, CVE-2021-37975, CVE-2021-37974, CVE-2021-37977, CVE-2021-37979, CVE-2021-37980, CVE-2021-37981, CVE-2021-37982, CVE-2021-37983, CVE-2021-37984, CVE-2021-37985, CVE-2021-37986, CVE-2021-37987, CVE-2021-37988, CVE-2021-37989, CVE-2021-37990, CVE-2021-37991, CVE-2021-37992, CVE-2021-37993, CVE-2021-37996, CVE-2021-37994, CVE-2021-37995, CVE-2021-38003, CVE-2021-38002, CVE-2021-38001, CVE-2021-38000, CVE-2021-37999, CVE-2021-37998 and CVE-2021-37997.

ISN 2021-09: Firefox ESR vulnerabilities

First published 30 November 2021

CVSS 3.1 Base Score: 10.0 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Summary

Several vulnerabilities have been found in Mozilla Firefox ESR, many rated as high. These affect the Firefox ESR version in the following IGEL products:

IGEL OS 11

IGEL OS 10

Details

Mozilla has reported various vulnerabilities in Firefox ESR in its Mozilla Foundation Security Advisories (MFSA-2021-49, MFSA-2021-45, MFSA-2021-40, MFSA-2021-37, MFSA-2021-33). Many concern memory safety, and many are exploitable over the network. Overall, 18 are rated high.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.06.210.
- IGEL OS 10: Upgrade to IGEL OS 11.06.210.

References

- MFSA-2021-49: https://www.mozilla.org/en-US/security/advisories/mfsa2021-49/
  CVE-2021-38503, CVE-2021-38504, CVE-2021-38506, CVE-2021-38507, MOZ-2021-0008, CVE-2021-38508, CVE-2021-38509, MOZ-2021-0007. (MOZ-* pending CVE assignment)
- MFSA-2021-45: https://www.mozilla.org/en-US/security/advisories/mfsa2021-45/
  CVE-2021-38496, CVE-2021-38497, CVE-2021-38498, CVE-2021-32810, CVE-2021-38500, CVE-2021-38501
- MFSA-2021-40: https://www.mozilla.org/en-US/security/advisories/mfsa2021-40/
  CVE-2021-38495
- MFSA-2021-37: https://www.mozilla.org/en-US/security/advisories/mfsa2021-37/
  CVE-2021-29991
- MFSA-2021-33: https://www.mozilla.org/en-US/security/advisories/mfsa2021-33/
  CVE-2021-29986, CVE-2021-29981, CVE-2021-29988, CVE-2021-29984, CVE-2021-29980, CVE-2021-29987, CVE-2021-29985, CVE-2021-29982, CVE-2021-29989, CVE-2021-29990

ISN 2021-08: ICG Authentication Vulnerability

First published 17 November 2021

CVSS 3.1 Base Score: 10.0 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Summary

A critical security vulnerability affects IGEL Cloud Gateway (ICG) in the following versions:

- All ICG versions before 2.04.100

Details

A penetration test has found an authentication vulnerability in ICG. It could enable an unauthenticated remote attacker to send commands and settings to connected IGEL OS endpoints.

IGEL would like to thank SCHUTZWERK GmbH, who discovered the vulnerability.

Update Instructions

- Update to ICG 2.04.100.

ISN 2021-07: UMS Web App Information Disclosure

First published 27 September 2021

CVSS 3.1 Base Score: 9.9 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:L

Summary

A critical security vulnerability in UMS Web App affects the following IGEL products:

- UMS 6.8.x with UMS Web App installed
- UMS 6.7.x with UMS Web App installed
- UMS 6.6.x with UMS Web App installed
- UMS 6.5.x with UMS Web App installed

Details

A penetration test has found that the UMS Web App can be made to reveal critical information, including the UMS Superuser password. IGEL would like to thank Lennert Preuth from SCHUTZWERK GmbH, who discovered the vulnerability.

Update Instructions

- Update to UMS 6.08.120

Mitigation

- IGEL strongly recommends that all affected users update/upgrade to UMS 6.08.120. If you have reasons not to do that, you can do the following:
    a. Make a UMS data backup.
    b. Re-run your current installer and re-install UMS without UMS Web App.

ISN 2021-06: IGEL OS OpenSSH Vulnerabilities

Updated 29 October 2021 (alternative mitigation for CVE-2020-15778)

Updated 23 September 2021 (IGEL OS 11.06.100 is now available)

First published 2 August 2021

CVSS 3.1 Base Score: 7.8 (High)

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

Three security vulnerabilities in OpenSSH affect the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

The `scp` command in OpenSSH through 8.3p1 allows command injection in the `scp.c toremote` function, as demonstrated by backtick characters in the destination argument (CVE-2020-15778). This allows `scp` users to execute commands on the remote system. Note: The vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows." This vulnerability is rated with a CVSS 3.1 Base Score 7.8 (High).

The ssh-agent in OpenSSH before 8.5 has a double free (CVE-2021-28041) that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system (does not apply to IGEL OS), or the forwarding of an agent to an attacker-controlled host. This vulnerability is rated with a CVSS 3.1 Base Score 7.1 (High). Also, the client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation (CVE-2020-14145). This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). Note: Some reports state that 8.5 and 8.6 are also affected. This vulnerability is rated with a CVSS 3.1 Base Score 4.3 (Medium).

Update Instructions

CVE-2021-28041 is fixed in IGEL OS 11.06.100.

There are no updates yet for the other two issues.

Mitigation

- The first option for CVE-2020-15778: Unless you explicitly need the OpenSSH server on IGEL OS, disable it. It is not needed for the management of IGEL OS endpoints via UMS or ICG.

1. In IGEL Setup, go to **System > Remote Access > SSH Access**.
2. Uncheck the **Enable** checkbox.
3. Click **Apply**.

4. Reboot the system.

- The second option for CVE-2020-15778: If you use the ssh server on IGEL OS for executing commands remotely, limit command execution via the `ssh` and `scp` commands:

1. In IGEL Setup, go to **System > Remote Access > SSH Access**.
2. Under **User access**, make sure that **user** is set to **Deny**.
3. Make sure that **ruser** is not denied access, and use **ruser** for ssh access.
4. Under **Applications access for remote user 'ruser'**, add a commandline with the full Linux path of the command you want to execute. Do this for every command you want to execute via ssh.
5. Click **Apply**.
6. Reboot the system.

- For CVE-2020-14145: If you offer an SSH client session to your IGEL OS users, instruct them to check the remote host key fingerprint on the first connect. Supply them with the correct fingerprint for comparison.

References

- CVE-2020-15778: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15778
- CVE-2021-28041: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28041
- CVE-2020-14145: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14145

ISN 2021-05: IGEL OS Denial of Service

Announced 23 July 2021

Updated 23 September 2021 (IGEL OS 11.06.100 is now available)

CVSS 3.1 Score: 8.8 (High)

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Summary

A local denial of service vulnerability affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

A research team from Qualys has discovered a vulnerability in `systemd` (CVE-2021-33910). An unprivileged local user can exploit it to crash `systemd` and the whole operating system (kernel panic).

Update Instructions

- IGEL OS 11: Upgrade to IGEL OS 11.06.100
- IGEL OS 10: Upgrade to IGEL OS 11

Mitigation

- Disable terminal access for the user, see *IGEL OS > Versions of IGEL OS > (11.09.310-en) IGEL OS > (11.09.310-en) IGEL OS Articles > (11.09.310-en) Security > (11.09.310-en) Security IGEL OS Endpoints > (11.09.310-en) Disabling Access to Components > (11.09.310-en) Disabling Local Terminal Access*.
- Disable virtual console access, see *IGEL OS > Versions of IGEL OS > (11.09.310-en) IGEL OS > (11.09.310-en) IGEL OS Articles > (11.09.310-en) Security > (11.09.310-en) Security IGEL OS Endpoints > (11.09.310-en) Disabling Access to Components > (11.09.310-en) Disabling Virtual Console Access*.
- As the attack relies on mounting user-controlled filesystems, disable mounting of filesystems by the user:
  - Disable storage hotplug (disabled by default), see *IGEL OS > Versions of IGEL OS > (11.09.310-en) IGEL OS > (11.09.310-en) IGEL OS Articles > (11.09.310-en) Security > (11.09.310-en) Security IGEL OS Endpoints > (11.09.310-en) Minimizing the Attack Surface > (11.09.310-en) Disabling Storage Hotplug*.
  - Remove the Mobile Device Access USB feature (removed by default), see *IGEL OS > Versions of IGEL OS > (11.09.310-en) IGEL OS > (11.09.310-en) IGEL OS Articles > (11.09.310-en) Security > (11.09.310-en) Security IGEL OS Endpoints > (11.09.310-en) Minimizing the Attack Surface > (11.09.310-en) Removing Unused Features*.

References

- Qualys, “CVE-2021-33910: Denial of Service (Stack Exhaustion) in systemd (PID 1))”: https://blog.qualys.com/vulnerabilities-threat-research/2021/07/20/cve-2021-33910-denial-of-service-stack-exhaustion-in-systemd-pid-1
- CVE-2021-33910: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33910

ISN 2021-04: IGEL OS Kernel Privilege Escalation

Announced 23 July 2021

Updated 23 September 2021 (IGEL OS 11.06.100 is now available)

CVSS 3.1 Score: 7.8 (High)

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

Summary

A local privilege escalation vulnerability affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

A research team from Qualys has discovered a vulnerability in the Linux kernel's filesystem layer (CVE-2021-33909). An unprivileged local user can use it to gain root privileges.

Update Instructions

- IGEL OS 11: Upgrade to IGEL OS 11.06.100
- IGEL OS 10: Upgrade to IGEL OS 11

Mitigation

- Disable terminal access for the user, see *IGEL OS > Versions of IGEL OS > (11.09.310-en) IGEL OS > (11.09.310-en) IGEL OS Articles > (11.09.310-en) Security > (11.09.310-en) Security IGEL OS Endpoints > (11.09.310-en) Disabling Access to Components > (11.09.310-en) Disabling Local Terminal Access*.
- Disable virtual console access, see *IGEL OS > Versions of IGEL OS > (11.09.310-en) IGEL OS > (11.09.310-en) IGEL OS Articles > (11.09.310-en) Security > (11.09.310-en) Security IGEL OS Endpoints > (11.09.310-en) Disabling Access to Components > (11.09.310-en) Disabling Virtual Console Access*
- As the attack relies on mounting user-controlled filesystems, disable mounting of filesystems by the user:
  - Disable storage hotplug (disabled by default), see *IGEL OS > Versions of IGEL OS > (11.09.310-en) IGEL OS > (11.09.310-en) IGEL OS Articles > (11.09.310-en) Security > (11.09.310-en) Security IGEL OS Endpoints > (11.09.310-en) Minimizing the Attack Surface > (11.09.310-en) Disabling Storage Hotplug.*
  - Remove the Mobile Device Access USB feature (removed by default), see *IGEL OS > Versions of IGEL OS > (11.09.310-en) IGEL OS > (11.09.310-en) IGEL OS Articles > (11.09.310-en) Security > (11.09.310-en) Security IGEL OS Endpoints > (11.09.310-en) Minimizing Attack Surface > (11.09.310-en) Removing Unused Features*.
- Qualys has published mitigations for the specific exploit that their researchers used (other exploitation techniques may exist): https://blog.qualys.com/vulnerabilities-threat-research/

2021/07/20/sequoia-a-local-privilege-escalation-vulnerability-in-linuxs-filesystem-layer-cve-2021-33909

References

- Qualys, “Sequoia: A Local Privilege Escalation Vulnerability in Linux’s Filesystem Layer (CVE-2021-33909)”: https://blog.qualys.com/vulnerabilities-threat-research/2021/07/20/sequoia-a-local-privilege-escalation-vulnerability-in-linuxs-filesystem-layer-cve-2021-33909
- CVE-2021-33909: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33909

ISN 2021-03: IGEL W10 Print Spooler Vulnerability

First published 7 July 2021
Updated 15 October 2021 (private build with security fixes available from IGEL)
Updated 16 July 2021 (inserted update instructions)

CVSS 3.1 Score: 8.8 (High)
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

A Remote Code Execution (RCE) vulnerability, known as PrintNightmare, affects the following IGEL products:

- IGEL W10 IoT

Details

A remote code execution vulnerability (CVE-2021-34527) exists when the Windows Print Spooler service improperly performs privileged file operations. An attacker who successfully exploited this vulnerability could run arbitrary code with SYSTEM privileges.

Update Instructions

1. IGEL customers can request the private build (PB) W10 IoT 4.04.180 from IGEL Customer Engineering (https://support.igel.com/csm), which contains the needed security fixes.
2. Install the update.
3. In addition to installing the update, in order to secure your system, you must confirm that the following registry settings are set to 0 (zero) or are not defined. In the default IGEL setting, they do not exist and therefore are in the secure setting already. You can check and set them by opening the Command Prompt and issuing the “regedit” command.
   - `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint`
   - `NoWarningNoElevationOnInstall = 0 (DWORD)` or `not defined` (default setting)
   - `UpdatePromptSettings = 0 (DWORD)` or `not defined` (default setting)

   Microsoft warns that having `NoWarningNoElevationOnInstall` set to “1” makes your system vulnerable by design.

References

- CVE-2021-34527: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34527
- Microsoft, “Windows Print Spooler Remote Code Execution Vulnerability”: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527
- Microsoft, “Windows Print Spooler Remote Code Execution Vulnerability”: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36958

ISN 2021-02: IGEL OS and W10 Wi-Fi Vulnerabilities (Fragattacks)

First published 21 May 2021

Updated 30 September 2021 (Resolution in IGEL OS 11.06.100)

CVSS 3.1 Score: 5.0 (Medium)
CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L

Several Wi-Fi vulnerabilities, known collectively as Fragattacks, affect the following IGEL products:

- IGEL OS 11
- IGEL OS 10
- IGEL W10 IoT

Details

The researcher Mathy Vanhoef has found several security vulnerabilities both in the IEEE 802.11 standards underpinning Wi-Fi and their implementations in Linux and Windows. He has demonstrated that weaknesses in the fragmentation and frame aggregation mechanisms can be abused to exfiltrate confidential data from or inject frames into a protected Wi-Fi connection between a client and the access point.

In IGEL software, these threats are mitigated as it uses TLS for endpoint management via UMS and ICG. Also, IGEL OS updates are cryptographically signed and validated. This is reflected in IGEL's CVSS 3.1 scoring of these issues.

Several CVE identifiers have been assigned to this group of vulnerabilities:

Design flaws:

- CVE-2020-24588[16]: Aggregation attack (accepting non-SPP A-MSDU frames)
- CVE-2020-24587[17]: Mixed key attack (reassembling fragments encrypted under different keys)
- CVE-2020-24586[18]: Fragment cache attack (not clearing fragments from memory when (re)connecting to a network)

Implementation vulnerabilities that allow the trivial injection of plaintext frames in a protected Wi-Fi network are assigned the following CVEs:

- CVE-2020-26140[19]: Accepting plaintext data frames in a protected network
- CVE-2020-26143[20]: Accepting fragmented plaintext data frames in a protected network

Other implementation flaws are assigned the following CVEs:

- CVE-2020-26147[21]: Reassembling mixed encrypted/plaintext fragments
- CVE-2020-26141[22]: Not verifying the TKIP MIC of fragmented frames.

16. https://nvd.nist.gov/vuln/detail/CVE-2020-24588
17. https://nvd.nist.gov/vuln/detail/CVE-2020-24587
18. https://nvd.nist.gov/vuln/detail/CVE-2020-24586
19. https://nvd.nist.gov/vuln/detail/CVE-2020-26140
20. https://nvd.nist.gov/vuln/detail/CVE-2020-26143
21. https://nvd.nist.gov/vuln/detail/CVE-2020-26147
22. https://nvd.nist.gov/vuln/detail/CVE-2020-26141

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.06.100 or newer. This fixes all design flaws and Linux implementation flaws listed above.
- IGEL OS 10: Upgrade to IGEL OS 11.06.100 or newer.

Mitigations

- If possible, replace Wi-Fi connections with wired Ethernet.

The reporter of these vulnerabilities recommends the following mitigations until fixes are available:

- Use HTTPS/TLS exclusively for websites in order to add another layer of protection for confidential information such as usernames and passwords.
  Keep your Wi-Fi access points updated with the latest firmware version.
- Reduce the impact of attacks by manually configuring your DNS server so that it cannot be poisoned.
- Specific to your Wi-Fi configuration, you can mitigate attacks (but not fully prevent them) by disabling fragmentation, disabling pairwise rekeys, and disabling dynamic fragmentation in Wi-Fi 6 (802.11ax) devices.

References

- https://www.fragattacks.com
- Mathy Vanhoef, “Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation”: https://papers.mathyvanhoef.com/usenix2021.pdf

ISN 2021-01: IGEL OS Remote Command Execution Vulnerability

Announced 25 February 2021

CVSS 3.1 Score: 9.8 (Critical)

A remote command execution (RCE) vulnerability affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

An external penetration test has found that the TLS connector service used in IGEL OS for *secure shadowing* and *secure terminal* is vulnerable to command injection. This vulnerability enables remote command execution in IGEL OS.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.04.270 or newer.
- IGEL OS 11.03.* branch: Update to version 11.03.620 or newer
- IGEL OS 10: Upgrade to IGEL OS 10.06.220 or newer.

Mitigation

Disable secure shadowing, see *IGEL OS > Versions of IGEL OS > (11.09.310-en) IGEL OS > (11.09.310-en) IGEL OS Reference Manual> (11.09.310-en) System > (11.09.310-en) Remote Access > (11.09.310-en) Shadow Settings in IGEL OS*. However, it is not advisable to use unencrypted shadowing instead.

Disable secure terminal, see I*GEL OS > Versions of IGEL OS > (11.09.310-en) IGEL OS > (11.09.310-en) IGEL OS Reference Manual> (11.09.310-en) System > (11.09.310-en) Remote Access > (11.09.310-en) Secure Terminal*.

ISN 2020-10: IGEL OS Bluetooth Vulnerabilities

Announced 8 December 2020

Score: High

Three Bluetooth vulnerabilities, one rated as high, affect the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

Weaknesses in input validation and access control have been discovered in BlueZ, the Linux Bluetooth stack, and have been nicknamed "BleedingTooth". CVE-2020-12352 and CVE-2020-24490, both rated medium, may disclose information to an unauthenticated user nearby. CVE-2020-12351 is rated high as it may allow an unauthenticated user nearby to enable escalation of privilege.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.04.240 or newer.
- IGEL OS 10: Upgrade to IGEL OS 11.

Mitigation

Disable Bluetooth, see I*GEL OS > Versions of IGEL OS > (11.09.310-en) IGEL OS > (11.09.310-en) IGEL OS Reference Manual> (11.09.310-en) Bluetooth Assistant.*

References

Intel BlueZ Advisory: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00435.html

ISN 2020-09: Command Execution from Start Menu

Announced 7 October 2020

Score: High

A local command execution security issue affects the start menu on:

- IGEL OS 11 (11.04.xxx before 11.04.130)

Details

A component update has added a feature to the start menu that lets unprivileged users run any command that the “User” account is allowed to execute. This enables users to break out of the limited user interface, e.g. to start a local terminal or add a session.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.04.130 or newer.

Mitigation

In IGEL Setup, go to **User Interface > Desktop > Start Menu** and set **Start menu type** to "Legacy". This removes command execution.

ISN 2020-08: Firefox ESR Various Vulnerabilities

Announced 17 September 2020

Score: High

Several security issues, 8 rated as high, affect the Firefox ESR web browser on:

- IGEL OS 11
- IGEL OS 10
- IGEL Linux 5

Details

It has been found that manipulating individual parts of a URL object could have caused an out-of-bounds read, leaking process memory to malicious JavaScript (CVE-2020-12418). Apart from that, by observing the stack trace for JavaScript errors in web workers, it was possible to leak the result of a cross-origin redirect (CVE-2020-15652. The WebRTC data channel could leak internal memory addresses to a peer, enabling them to bypass ASLR (CVE-2020-6514).
Another vulnerability allowed a malicious webpage to prompt the user to install an extension. Combined with user confusion, this could result in an unintended or malicious extension being installed (CVE-2020-15664).
Finally, a number of memory management bugs have been discovered (CVE-2020-12419, CVE-2020-12420, CVE-2020-15659, CVE-2020-15669).

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.04.130 or newer.
- IGEL OS 10: An updated version is upcoming. When it is available, this document will be updated.
- IGEL Linux 5: This version does not have the space required for the Firefox ESR update. IGEL recommends removing the web browser feature if possible: https://wiki.test.toolchain.igel.kreuzwerker.net/igellinux/en/features-2275613.html

References

Mozilla Foundation Security Advisory 2020-25: https://www.mozilla.org/en-US/security/advisories/mfsa2020-25/

Mozilla Foundation Security Advisory 2020-31: https://www.mozilla.org/en-US/security/advisories/mfsa2020-31/

Mozilla Foundation Security Advisory 2020-37: https://www.mozilla.org/en-US/security/advisories/mfsa2020-37/

ISN 2020-07: Firefox ESR Various Vulnerabilities

Announced 9 June 2020

Score: High

Four security issues rated as high affect the Firefox ESR web browser on:

- IGEL OS 11
- IGEL OS 10
- IGEL Linux 5

Details

It has been discovered that a timing attack against Mozilla's Network Security Services (NSS) library could leak private keys (CVE-2020-12399). Also, when browsing a malicious page, a race condition in SharedWorkerService could occur and lead to a potentially exploitable crash (CVE-2020-12405). A JavaScript type confusion with NativeTypes could result in a crash, and potentially to execution of arbitrary code (CVE-2020-12406). Further memory safety bugs showed evidence of memory corruption and Mozilla presume that with enough effort some of these could have been exploited to run arbitrary code (CVE-2020-12411).

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.03.580 or newer.
- IGEL OS 10: Update to IGEL OS 10.06.190 or newer.
- IGEL Linux 5: This version does not have the space required for the Firefox ESR update. IGEL recommends removing the web browser feature if possible.

References

Mozilla Foundation Security Advisory 2020-21: https://www.mozilla.org/en-US/security/advisories/mfsa2020-21/

ISN 2020-06: IGEL Cloud Gateway (ICG) Various Vulnerabilities

Announced 15 July 2020

Score: High

Various security issues, among them 3 rated as high, have been discovered in IGEL Cloud Gateway (ICG) before version 2.02.100.

Details

A penetration test commissioned by IGEL has found an issue in the authentication mechanism between UMS and ICG. Furthermore, there were some missing or not strict enough authorization checks in the communication between UMS, ICG and the endpoint devices. Finally, there was information disclosure in the server status response and in the ICG log files.

Update Instructions

- Update to IGEL Cloud Gateway 2.02.100 or newer.

ISN 2020-05: Intel Chipset Vulnerabilities

Announced 9 June 2020

Score: Medium

A vulnerability in Intel chipsets affects the following IGEL hardware:

- IGEL UD 2 (M250C) with BIOS versions before v3.D.13-05292019 (July 2019)
- IGEL UD 6 (H830C) with BIOS versions before v.3.3.13-05232019 (July 2019)

Details

A potential security vulnerability in Intel CPUs may allow information disclosure.

Update Instructions

IGEL OS users need not update the BIOS/UEFI. Instead, the microcode released by Intel will be applied at boot time by IGEL OS.

- IGEL OS 11: Update to IGEL OS 11.03.580 or newer
- IGEL OS 10: Update to IGEL OS 10.06.180 or newer

References

INTEL-SA-00233 “Microarchitectural Data Sampling Advisory”: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00233.html

ISN 2020-04: Firefox ESR Various Vulnerabilities

Announced 9 June 2020

Score: Critical

Two security issues rated critical and one rated high affect the Firefox ESR web browser on

- IGEL OS 11
- IGEL OS 10
- IGEL Linux 5

Details

A race condition when running shutdown code for Web Worker led to a use-after-free vulnerability. This resulted in a potentially exploitable crash. (CVE-2020-12387). Additionally, memory safety bugs have been reported in Firefox ESR 68.7. Some of these bugs showed evidence of memory corruption and Mozilla presume that with enough effort some of these could have been exploited to run arbitrary code (CVE-2020-12395). Furthermore, a buffer overflow could occur when parsing and validating SCTP chunks in WebRTC. This could have led to memory corruption and a potentially exploitable crash (CVE-2020-6831).

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.03.580 or newer.
- IGEL OS 10: Update to IGEL OS 10.06.180 or newer.
- IGEL Linux v5: This version does not have the space required for the Firefox ESR update. IGEL recommends removing the web browser feature if possible.

References

Mozilla Foundation Security Advisory 2020-17: https://www.mozilla.org/en-US/security/advisories/mfsa2020-17/

ISN 2020-03: Firefox ESR Vulnerabilities

Announced 24 April 2020

Score: Critical

Two critical security issues affect the Firefox ESR web browser on

- IGEL OS 11
- IGEL OS 10
- IGEL Linux 5

Details

Under certain conditions, when running the nsDocShell destructor (CVE-2020-6819) or when handling a ReadableStream (CVE-2020-6820), race conditions can cause a use-after-free. These vulnerabilities can be exploited to inject code into Firefox memory and execute it in the web browser's context. Mozilla are aware of targeted attacks in the wild abusing these flaws.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.03.530 or newer.
- IGEL OS 10: Update to IGEL OS 10.06.179 or newer.
- IGEL Linux 5: This version does not have the space required for the Firefox ESR update. IGEL recommends removing the web browser feature if possible.

References

Mozilla Foundation Security Advisory 2020-11: https://www.mozilla.org/en-US/security/advisories/mfsa2020-11/

ISN 2020-02: Windows CryptoAPI Spoofing Vulnerability

Announced 24 February 2020

Score: High

A high scoring security issue affects IGEL Windows 10 IoT

Details

A vulnerability has been discovered in the way Windows CryptoAPI (Crypt32.dll) validates Elliptic Curve Cryptography (ECC) certificates (CVE-2020-0601). An attacker could exploit this to sign a malware executable with a spoofed certificate so that it will look legitimate to Windows. This vulnerability is also known as “Curve Ball” or “Chain of Fools”.

Update Instructions

- Update to IGEL Windows 10 IoT version 4.04.140 or newer.

References

NVD - CVE-2020-0601 Detail: https://nvd.nist.gov/vuln/detail/CVE-2020-0601

ISN 2020-01: Firefox ESR Vulnerability

Announced 15 January 2020

Score: Critical

A critical security issue affects the Firefox ESR web browser on

- IGEL OS 11
- IGEL OS 10
- IGEL Linux 5

Details

Incorrect alias information in IonMonkey JIT compiler for setting array elements could lead to a type confusion (memory vulnerability). Mozilla is aware of targeted attacks in the wild abusing this flaw (CVE-2019-17026).

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.03.110 or newer.
- IGEL OS 10: Update to IGEL OS 10.06.170 or newer.
- IGEL Linux 5: This version does not have the space required for the Firefox ESR update. IGEL recommends removing the web browser feature if possible.

References

Mozilla Foundation Security Advisory 2020-03: https://www.mozilla.org/en-US/security/advisories/mfsa2020-03/

ISN-2019-13: Windows Defender

Announced 17 October 2019

Score: High

A security issue affects IGEL Windows products in the following versions:

- IGEL Windows 10 IoT

Details

A denial of service vulnerability exists when Microsoft Defender improperly handles files. An attacker could exploit the vulnerability to overwrite the discretionary access control list (DACL) for a file. To exploit the vulnerability, an attacker would first require execution on the victim system.

Update Instructions

- IGEL Windows 10 IoT: Update to IGEL Windows 10 IoT 4.04.120 or newer.

References

Microsoft Security Response Center - CVE-2019-1255 | Microsoft Defender Denial of Service Vulnerability: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1255

ISN-2019-12: Internet Explorer Vulnerability

Announced 08 October 2019

Score: High

A security issue affects IGEL Windows products in the following versions:

- Universal Desktop W7+
- IGEL Windows 10 IoT

Details

A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user.

Update Instructions

- Universal Desktop W7+: Update to version 3.14.100 or newer.
- IGEL Windows 10 IoT: Upgrade to IGEL Windows 10 IoT 4.04.120 or newer.

References

Microsoft Security Response Center - CVE-2019-1367 | Scripting Engine Memory Corruption

Vulnerability: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1367

ISN 2019-11: Firefox ESR Vulnerabilities

.Announced 13 September 2019

Score: High

Several security issues affect the Firefox ESR web browser on

- IGEL OS 11
- IGEL OS 10
- IGEL Linux v5

Details

Many vulnerabilities have been discovered in Firefox ESR, which Mozilla has summarized in the Mozilla Foundation Security Advisory (MFSA) 2019-27 with an overall critical score. The advisory contains CVE-2019-11746, CVE-2019-11744, CVE-2019-11752, CVE-2019-9812, CVE-2016-11743 and CVE-2019-11740, which include potentially exploitable crashes while manipulating video elements or extracting a key value in IndexedDB, and a sandbox escape through Firefox Sync.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.02.150 or newer.
- IGEL OS 10: Update to IGEL OS 10.06.130 or newer.
- IGEL Linux 5: This version does not have the space required for the Firefox ESR update. IGEL recommends removing the web browser feature if possible.

References

Mozilla Foundation Security Advisory 2019-27: https://www.mozilla.org/en-US/security/advisories/mfsa2019-27/

ISN 2019-10: Spectre SWAPGS CPU Vulnerability

Announced 16 August 2019

Score: Low

A security issue affects Intel and AMD x86_64 CPUs.

Details

A Spectre-v1-like vulnerability using the "SWAPGS" instruction (CVE-2019-1125) has been discovered in 64-bit CPUs. It could enable a skilled local attacker to access private information via a side channel attack. This vulnerability can be mitigated by operating system updates.

IGEL assigns only a score of "Low" to this vulnerability because on IGEL operating systems there is only one non-privileged user that owns private information. A scenario of another non-privileged user using this attack to access private data is therefore not realistic.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.02.150 or newer (an earlier fix in IGEL OS 11.02.100 contains a backporting error, CVE-2019-15902).
- IGEL OS 10: Update to IGEL OS 10.06.120 or newer.
- IGEL Windows 10 IoT: Upgrade to IGEL Windows 10 IoT 4.04.110 or newer.
- Universal Desktop W7+: Update to Universal Desktop W7+ version 3.13.150 or newer.

References

Bitdefender: SWAPGS Attack: https://www.bitdefender.com/business/swapgs-attack.html

Red Hat Knowledgebase: CVE-2019-112: Spectre SWAPGS gadget vulnerability: https://access.redhat.com/articles/4329821

ISN 2019-09: IGEL OS SWP Vulnerability

Announced 24 July 2019

Score: High

A security issue affects the Shared Workplace (SWP) feature in the following IGEL OS version:

- IGEL OS 10.06.100

Details

The Shared Workplace login accepts any user credentials. However, no user settings are applied to the device.

Update Instructions

- Update to IGEL OS 10.06.110 or newer.

ISN 2019-08: Firefox ESR Vulnerabilities

Announced 24 July 2019

Score: Critical

Several security issues affect the Firefox ESR web browser on

- IGEL OS 11
- IGEL OS 10
- IGEL Linux v5

Details

Many vulnerabilities have been discovered in Firefox ESR, which Mozilla has summarized in the following Mozilla Foundation Security Advisories (MFSAs): MFSA-2019-22, MFSA-2019-19, MFSA- 2019-18, MFSA-2019-08, MFSA-2019-05 and MFSA-2019-02. Among these are vulnerabilities such as a sandbox escape, a script injection vulnerability, privilege escalation and some critical memory management weaknesses.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.01.130 or newer.
- IGEL OS 10: Update to IGEL OS 10.06.110 or newer.

Mitigation

- IGEL Linux 5: This version does not have the space required for the Firefox ESR update. IGEL recommends disabling the web browser feature if possible.

References

- MFSA-2019-22: https://www.mozilla.org/en-US/security/advisories/mfsa2019-22/
- Mozilla Foundation Security Advisories: https://www.mozilla.org/en-US/security/advisories/

ISN 2019-07: Firefox ESR Vulnerability

Announced 5 July 2019

Score: High

A security issue affects the Firefox ESR web browser on

- IGEL OS 11
- IGEL OS 10
- IGEL Linux 5

Details

Two vulnerabilities (CVE-2019-11708 and CVE-2019-11707) have been discovered in Firefox that in combination allow a remote attacker to execute code on a target machine.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.01.120, containing the fixed Firefox ESR version 60.7.2.
- IGEL OS 10: Update to IGEL OS 10.05.830, containing the fixed Firefox ESR version 60.7.2.

Mitigation

- IGEL Linux 5: This version does not have the space required for the Firefox ESR update. IGEL recommends disabling the web browser feature if possible.

ISN 2019-06: IGEL OS Kernel Vulnerability

Announced 5 July 2019

Score: High

A security issue affects IGEL Linux-based operating systems in the following versions:

- IGEL OS 11
- IGEL OS 10
- IGEL Linux 5

Details

It has been discovered that the Linux Kernel can be crashed by sending specially crafted network packets to a Linux host (CVE-2019-11477, CVE-2019-11478 and CVE-2019-11479). Issues in minimum segment size (MSS) and TCP Selective Acknowledgement (SACK) capabilities can cause a kernel panic.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.01.120
- IGEL OS 10: Update to IGEL OS 10.05.830

Mitigation

- IGEL Linux 5: Add the following command to **System > Firmware Customization > Custom Commands > Base > Initialization**: `echo 0 > /proc/sys/net/ipv4/tcp_mtu_probing ; iptables -I INPUT -p tcp -m tcpmss --mss 1:1000 -j DROP`

References

Advisory from Netflix with further suggestions for workarounds:

https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-001.md

ISN 2019-05: UMS HA Vulnerability

Announced 14 June 2019

Score: High

A security issue affects Universal Management Suite (UMS) in the following versions:

- UMS 5.x if using High Availability feature
- UMS 6.x if using High Availability feature

Details

It has been discovered that a UMS component used for the High Availability (HA) feature has a debug port open. This may enable a remote attacker to read information and execute Java code in the context of the Java VM.

Update Instructions

Update to UMS 6.02.100 or newer.

To update your UMS installation, please follow these instructions: *Universal Management Suite > (12.04-en) Universal Management Suite > (12.04-en) Universal Management Suite (UMS) > (12.04-en) UMS Reference Manual > (12.04-en) UMS Installation and Update > (12.04-en) IGEL UMS Update*.

ISN 2019-04: RDP Vulnerability in WES7

Announced 7 June 2019

Score: Critical

A security issue in Remote Desktop Services affects IGEL Windows Embedded Standard 7 (WES7) in all versions.

Details

Microsoft has reported a remote code execution vulnerability (CVE-2019-0708, KB4499175) in Remote Desktop Services (formerly known as Terminal Services) affecting many Windows versions up to 7. An unauthenticated attacker can remotely install programs, view, change, or delete data, or create new accounts with full user rights. This requires no user interaction and could therefore be exploited by a worm – this is why this vulnerability scores as critical.

Update Instructions

Update all your IGEL Windows Embedded Standard 7 systems to version 3.13.140.

Further Information

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

ISN 2019-03: Zombieload, RIDL, Fallout

Announced 22 May 2019

Score: Low

A security issue affects Intel-based devices running the following IGEL software products:

- IGEL OS 11
- IGEL OS 10
- IGEL Windows 10 Enterprise IoT

Details

Several vulnerabilities (CVE-2018-12126, CVE-2018-12130, CVE-2018-12127, CVE-2019-11091) affect the speculative execution features of Intel microprocessors. They can enable an attacker's code to read data from other parts of the processor, which by design should be inaccessible to it. In principle, this would allow stealing information from a different process, user or virtual machine.

However, IGEL operating systems do not run virtual machines, do not support multi-user operation and do only run preinstalled code from a read-only file system. Therefore, the impact on IGEL operating systems is low.

Update Instructions

IGEL is preparing IGEL OS 11, IGEL OS 10 and IGEL W10 firmware versions with security fixes. This ISN will be updated to inform customers when these versions become available.

IGEL W10 4.04.100 (upcoming)

IGEL OS 10 10.06.100 (upcoming)

IGEL OS 11 11.02.100 (upcoming)

ISN 2019-02: UMS Vulnerability

Overview

Announced 24 April 2019

Score: High

A security issue affects Universal Management Suite (UMS) in the following versions:

- UMS 6.x
- UMS 5.x

Details

An implementation bug in UMS user authentication allows an unauthenticated user to send commands to devices.

Update Instructions

UMS 6.x

Update to UMS 6.01.130 or newer. For instructions, see *Universal Management Suite > (12.04-en) Universal Management Suite > (12.04-en) Universal Management Suite (UMS) > (12.04-en) UMS Reference Manual > (12.04-en) UMS Installation and Update > (12.04-en) IGEL UMS Update*.

UMS 5.x

Update to UMS 5.09.140 or newer. For instructions, see *Universal Management Suite > (12.04-en) Universal Management Suite > (12.04-en) Universal Management Suite (UMS) > (12.04-en) UMS Reference Manual > (12.04-en) UMS Installation and Update > (12.04-en) IGEL UMS Update*.

ISN 2019-01: UMS Vulnerability

Overview

Announced 28 March 2019

Severity: High

A security issue affects Universal Management Suite (UMS) in the following versions:

* UMS 6.x

* UMS 5.x

Details

An implementation bug in endpoint authentication allows an endpoint to impersonate another endpoint when communicating with UMS.

IGEL would like to thank Timo Lindfors from Nixu Corporation who discovered and reported this.

Update Instructions

UMS 6.x: Update to UMS 6.01.110 or newer.

UMS 5.x: Update to UMS 5.09.130 or newer.

To update your UMS installation, please follow these instructions: *Universal Management Suite > (12.04-en) Universal Management Suite > (12.04-en) Universal Management Suite (UMS) > (12.04-en) UMS Reference Manual > (12.04-en) UMS Installation and Update > (12.04-en) IGEL UMS Update*.

ISN 2023-25: Webkit Vulnerabilities

Updated 19th October 2023 (Citrix Self-Service compatibility)

First published 18th October 2023

CVSS 3.1: 9.8 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

Multiple vulnerabilities have been discovered in the Webkit browser engine. This affects the following IGEL products:

- IGEL OS 12
- IGEL OS 11

Details

Multiple vulnerabilities have been found in Webkit. They could allow a remote attacker to execute arbitrary code on the local operating system when the user visits malicious web content. One vulnerability (CVE-2023-41993) is graded as critical, and Apple is aware of a report that it may have been actively exploited. The other two issues (CVE-2023-39928, CVE-2023-41074) are graded as high.

Update Instructions

- OS 12: Update to OS 12 base system version 12.2.1 (scheduled for 26 October 2023)
- OS 11: Update to OS 11.09.110

> For compatibility reasons with Citrix Self-Service, the Citrix Workspace App in OS 11.09.110 uses older Webkit that suffers from these vulnerabilities. However, the risk is mitigated by the fact that Citrix Self-Service does not open arbitrary web pages, but only pages from the customer's Citrix infrastructure. The rest of the system uses the updated Webkit with the security fixes.

References

- CVE-2023-41993: https://nvd.nist.gov/vuln/detail/CVE-2023-41993
- CVE-2023-39928: https://nvd.nist.gov/vuln/detail/CVE-2023-39928
- CVE-2023-41074: https://nvd.nist.gov/vuln/detail/CVE-2023-41074

IGEL OS 12 Hardening Guide

Introduction

This article explains how to apply security-focused settings to IGEL OS 12 devices to improve endpoint protection. The recommendations apply to a variety of device types and deployment scenarios.

System Environment

- IGEL OS Version: IGEL OS 12 or later
- Supported Deployment Types:
  - Devices with IGEL OS 12 pre-installed by the hardware vendor
  - Devices permanently installed using:
    - IGEL OS 12 Creator (OSC)
    - IGEL OS 12 Base System Image (PXE boot) or
    - IGEL OS 12 Deployment Tool (SCCM)
  - Devices temporarily converted using UD Pocket

Security Introduction

This article describes various configuration settings designed to enhance the security of IGEL OS 12. In general, applying more of these settings will result in stronger device security. However, you must balance security requirements and operational needs. For example, disabling Bluetooth may be counterproductive in environments where Bluetooth peripherals are required.

To manage security across multiple devices, configure the relevant settings in **Universal Management Suite (UMS) Priority Profiles** and assign them accordingly.

For more information, see Priority Profiles in the IGEL UMS[23].

23. https://kb.igel.com/en/universal-management-suite/current/priority-profiles-in-the-igel-ums

Setting Passwords

You can restrict access to various system components by setting passwords.

Setting an Administrator Password

Rationale

Passwords protect the system against local changes. They restrict access to the Local Terminal, Setup, and to the rescue shells on the virtual consoles. The administrator password is also needed to reset the system to factory defaults.

These passwords are stored in a secure format (salted and hashed) and cannot be recovered from local storage.

By default, no passwords are set on IGEL OS. Set at least an administrator password.

Instructions

1. In IGEL Setup, go to `Security > Password`.
2. In the **Administrator** area, check **Use Password**.
3. Enter a password twice when prompted.
4. Click **Set password**.
5. (Optional) If you want to grant an unprivileged user access to IGEL Setup, check **Use Password** in the **Setup user** area and enter a password twice when prompted. Click **Set password**.
6. Click **Save**.

Enforcing User Authentication at the Device

Rationale

You can configure your device to require authentication by the user on each system start. This is possible both for the local user and for an Active Directory (AD) or SSO user.

Instructions

The following instructions describe the configuration for the local user. For Active Directory or an SSO Identity Provider, as well as other logon topics, see: Logon Settings in IGEL OS 12[24].

⚠ Do not activate **Security > Logon > Guest,** as this allows access to IGEL OS 12 without authentication. This is not suitable for secure environments.

1. Go to **Security > Password** and activate **Use Password** for the **Local User**. You are prompted to enter a password.
2. Go to **System > Registry > auth > login > xlock** and activate **Login with Local User password**.
3. (Optional) If you want a screen lock after a defined time of inactivity:
    - Go to **User Interface > Screenlock / Screensaver > Options**.
    - Activate **Start automatically**.
    - Set **Timeout** to the desired time of inactivity (in minutes).
    - Activate **Require password to unlock (screenlock)**.
4. Click **Save**.

24. https://kb.igel.com/en/igel-os-base-system/current/logon-settings-in-igel-os-12

Password-Protecting Sessions and Accessories

Rationale

Sessions can be used to access corporate resources, while the accessories in IGEL OS can be used to make changes to the local system. If you do not want to disable certain sessions or accessories completely, you can set passwords to restrict access to them.

Instructions

By default, sessions do not have passwords set. In IGEL Setup, you can set a password on the **Starting Methods for Session** page of a session or accessory.

To enable password protection:

1. In the Setup, go to the relevant **Starting Methods for Session** page. The path has the following pattern:
   Sessions > [session type] > [session name]
   For accessories, go to: **Accessories > [accessory name]**
2. Set **Password Protection** to one of the following:
   - **Administrator** – requires the Administrator password
   - **User** – requires the Local User password
   - **Setup User** – requires the Setup User password
3. Click **Save**.

Using Screenlock

Rationale

Leaving a screen unlocked enables attackers to access the system with the logged-in user's privileges. Manually or automatically locking the screen with a password helps prevent unauthorized access.

Instructions for Enabling Manual and Automatic Locking

By default, there is no way for the user to manually lock the screen. To enable manual and automatic screen locking, follow these steps:

1. In Setup, go to **User Interface > Screenlock / Screensaver > Options**.
2. Activate the **Screenlock Session**.
3. Activate the **Quick Start Panel** starting method to provide a manual lock button to the user.
4. Activate **Password Protection** and set it to **User**.
5. Activate **Hotkey Configuration** and assign a key combination to lock the screen manually (e.g., **[Ctrl|Shift+L]**).
6. Go to the **Options** section.
7. Activate **Start automatically**.
8. (Optional) Adjust the **Timeout** to the desired idle time (in minutes).
9. Click **Save**.

Setting a UEFI Password

Rationale

In the UEFI settings, you can modify fundamental system properties, e.g. enabling Secure Boot or disabling USB boot. Access to these settings should be protected with a password to prevent unauthorized changes.

Instructions for IGEL Devices

→ If UEFI Secure Boot is not enabled, see the instructions under UEFI Secure Boot Enabling Guides[25].

By default, no UEFI password is set on IGEL UD devices. To set a password:

1. Hold down the [Del] key ([F2] for UD2 devices) while booting.
   The UEFI menu opens.
2. Use the arrow and return keys to navigate to **SCU**.
   The Setup Utility opens.
3. Navigate to the **Security** section.
4. Select **Set Supervisor Password** using the arrow keys.
5. Press [Return].
6. Enter the desired UEFI password and press [Return].
7. Re-enter the same password and press [Return] twice.
8. Press [F10] to save and exit.
9. Confirm **Exit Saving Changes?** by pressing [Return].

The system will reboot, and UEFI settings are now password-protected.

Instructions for 3rd-Party Devices Converted with OS Creator (OSC)

→ Refer to the instructions of your BIOS/UEFI vendor.

25. https://kb.igel.com/en/security-safety/current/uefi-secure-boot-enabling-guides

Using Two-Factor Authentication (2FA)

Rationale

Two-factor authentication (2FA) combines two different factors to verify a user's identity. In addition to a password or PIN, this can include a smart card, hardware token, or smartphone app. This improves protection against impostors, as they must possess both the physical device (or smartphone) and knowledge of the password or PIN.

Single Sign On Providers

- If you are using one of the Identity Providers supported by IGEL OS 12 (Entra ID, Ping Identity, Okta, VMware Workspace ONE Access) for device login, you can enable the 2FA options offered by those providers — typically using a smartphone app.
  --> Refer to the documentation provided by your SSO provider.
- These Identity Providers can also be used to:
  - Unlock the Screenlock
  - Authenticate remote sessions

--> For details, see: How to Configure Single Sign-On (SSO) on IGEL OS 12[26]

Use Smart Card and Smart Key Authentication

- IGEL OS 12 also supports smart card and smart key authentication.
- See the following articles for setup details:
  - Smartcard Services in IGEL OS 12[27]
  - How to Use Smart Card and Smart Key Authentication[28]

26. https://kb.igel.com/en/igel-os-base-system/current/how-to-configure-single-sign-on-sso-on-igel-os-12
27. https://kb.igel.com/en/igel-os-base-system/current/smartcard-services-in-igel-os-12
28. https://kb.igel.com/en/igel-os-base-system/current/how-to-use-smart-card-and-smart-key-authentication

How to Keep the System Up-To-Date

Rationale

Software updates fix newly discovered vulnerabilities in the IGEL OS Base System and the installed apps. Keeping up with updates is one of the most important measures for securing IGEL OS systems.

⚠ Always test new IGEL OS 12 and app versions in a controlled test environment before deploying them in production.

Instructions

Follow the official guide: How to Keep Your IGEL OS 12 System Up to Date[29].

29. https://kb.igel.com/en/igel-os-base-system/current/how-to-keep-your-igel-os-12-system-up-to-date

Disabling Access to Components

You can hide IGEL OS components from the user that could be used to make changes to the system

Disabling Local Terminal Access

The Local Terminal accessory allows the user to execute commands or make changes to the system. By default, the local terminal is disabled; that is, no local terminal session is configured. To enhance security, you should do one of the following:

- Leave the local terminal disabled.
- If a local terminal session is configured but not needed, disable it.
- If a local terminal session is needed, password-protect it.

Instructions

To remove an existing local terminal session:

1. In IGEL Setup, go to **Accessories > Terminals**.
2. Select the local terminal session you want to delete.
3. Click the trash icon to remove the selected session.
4. When prompted, confirm that you want to delete the session.
5. Click **Save**.

To password-protect the local terminal session:

1. Find the local terminal session under **Accessories > Terminals**.
2. Set the **Password Protection** field to **Administrator** to restrict access from normal users.

Disabling Virtual Console Access

Rationale

The virtual consoles `tty11` and `tty12` allow the user to access a shell. Disabling these consoles makes it more difficult to execute commands or make unauthorized changes to the system.

Instructions

By default, the user can access the virtual consoles using the [Ctrl]+[Alt]+[F11] and [Ctrl]+[Alt]+[F12] key combinations. To disable this access:

1. In IGEL Setup, go to **User Interface > Display Settings > Access Control**.
2. Activate **Disable Console Switching**
   (Default: Console switching enabled).
3. Click **Save**.

Hiding Unused Accessories

Rationale

Accessories can be used to make changes to the system. Restricting access to unused accessories helps to keep the system secure.

Instructions

To hide individual accessories:

1. In IGEL Setup, go to **Accessories > [accessory name]**.
2. Disable all **Starting Methods for Session**.
3. Click **Save**.

To password-protect an accessory:

1. Go to the **Starting Methods for Session** section.
2. Activate **Password Protection**.
3. Select **Administrator** to restrict access from regular users.

To hide the entire Application Launcher's System page:

1. In IGEL Setup, go to **Accessories > Application Launcher > Application Launcher Configuration**.
2. Activate **Hide system page**.
3. Click **Save**.

Use Strong Device Encryption Settings

Rationale

To strengthen the security of your endpoint device, you can deploy strong device encryption. The encryption is applied to all partitions that can contain user data, for example, browser history or the general configuration directory `/wfs`.

Instructions

1. In Setup, go to **Security > Device Encryption**.
2. If your device supports TPM 2.0, use it to protect the encryption key:
    - The **TPM+PIN** mode is widely supported.
    - **TPM PCR** and **TPM PCR+PIN** are only supported on selected hardware.

For full details, see: Device Encryption in IGEL OS 12[30]

30. https://kb.igel.com/en/igel-os-base-system/current/device-encryption-in-igel-os-12

Minimizing the Attack Surface

Secure App Choices

Installing and running software from untrusted sources puts system and data security at risk. IGEL OS helps protect devices by only accepting cryptographically signed app packages.

IGEL considers the following app sources secure. Their signatures are accepted by IGEL OS by default:

- IGEL-built apps from [app.igel.com[31]]
  (Author: IGEL Technology GmbH)
- Apps from IGEL Ready developers from [app.igel.com[32]]
  (Built by IGEL Ready partners and security-reviewed by IGEL)

Use caution when working with apps from the IGEL App Creator Portal[33]:

- Apps you build yourself
  If you use a script from the community, review the script and verify which binaries it downloads and from where.
- Apps built by a trusted contact
  Trust decisions about App Creator Portal users are at your discretion.

To use these apps securely:

- Import the app creator's certificate into UMS as a file of type **App Signing Certificate**.
- Assign the certificate file to the target device(s) to allow IGEL OS to trust apps signed with that certificate.

For instructions, see: Registering Files on the IGEL UMS Server[34]

31. http://app.igel.com
32. http://app.igel.com
33. https://appcreator.igel.com
34. https://kb.igel.com/en/universal-management-suite/12.06.120/files-registering-files-on-the-igel-ums-server-and

Using Browser Kiosk Mode

When possible, configure browser-only workstations to use Chromium in kiosk mode.

To learn how to activate kiosk mode and review additional hardening options for the Chromium browser, see: Configuration of the Chromium Browser in IGEL OS[35].

35. https://kb.igel.com/en/igel-apps/current/configuration-of-the-chromium-browser-in-igel-os#ConfigurationoftheChromiumBrowserinIGELOS-ConfiguringGlobalSettings

Disabling the PC/SC Daemon

Rationale

Unless you are using smartcard readers that depend on it, you can safely disable the PC/SC daemon. Reducing the number of active daemons helps minimize the system's attack surface.

Instructions

To deactivate the PC/SC daemon:

1. In IGEL Setup, go to **Security > Smartcard > Services**.
2. Deactivate **Activate PC/SC Daemon**.
3. Click **Save**.

Disabling X Server TCP Connections

Rationale

The X graphics server in IGEL OS includes network functionality that, if enabled, could allow others to view your screen or capture keyboard input. Keeping this feature disabled helps maintain the confidentiality of user data.

Instructions

By default, the network functionality of the X server is disabled. To ensure it remains disabled (or to disable it again later), follow these steps:

1. In IGEL Setup, go to **User Interface > Display > Access Control**.
2. Ensure that **Access Control** is activated.
3. Ensure that **Disable TCP Connections** is activated.
4. Click **Save**.

Disabling RPC Portmapper Service

Rationale

By default, IGEL OS 12 runs the RPC portmapper service on port 111 (TCP and UDP) to help other hosts discover services such as CUPS, NFS, or SMB that it may be running.
Since these services are typically not required on most endpoints, you can safely stop the RPC portmapper service to reduce the attack surface.

Instructions

1. In Setup, go to **System > System Customization > Custom Commands > Network.**
2. Enter the following commands into the **Final network command** field to stop the RPC portmapper service:

   ```
   systemctl stop rpcbind.socket
   systemctl stop rpcbind.service
   ```

3. Click **Save**.

Disabling Storage Hotplug

Rationale

Removable USB storage media can be used to steal data, execute unauthorized software, or introduce malware onto the device.

Instructions

Storage hotplug is disabled by default. If you need to disable it again later, follow these steps:

1. In IGEL Setup, go to **Devices > Storage Devices > Storage Hotplug**.
2. Deactivate **Enable Dynamic Client Drive Mapping**.
3. Click **Apply**.

After this change, storage devices will no longer be automatically mounted when they are plugged in.

Using USB Device Control

Rationale

USB devices such as pen drives, wireless controllers, or printers can be used to steal data, execute unauthorized software, or introduce malware. Disabling or restricting as many USB device classes as possible significantly improves system security.

Instructions

To enable and configure USB access control:

1. In IGEL Setup, go to **Devices > USB Access Control**.
2. Activate **Enable**.

> Activating USB Access Control and setting the **Default rule** to **Deny** will block all USB devices locally and in sessions. This may also disable devices required by users.
> → Enable USB Access Control only if your security policy requires it. In that case, set **Default rule** to **Deny** and configure **Allow** rules for the necessary USB devices or classes.
> **Recommendation:** Configure USB Access Control as the final step of your device setup. Before activating it, verify that all configurations for printers, unified communications, USB redirection, and device mappings function as intended.
> **Note:**
> - USB Access Control is completely separate from USB Redirection used in remote sessions. For guidance, see When to Use USB Redirection[36].
> - This feature does not physically disable a USB port, i.e power delivery will still function.

3. Set **Default rule** to **Deny**.

   In combination with the preconfigured rule allowing **Human Interface Devices (HID)**, only essential peripherals such as the mouse and keyboard will remain functional.

4. Configure additional rules as needed.
   For details, see USB Access Control in IGEL OS 12[37].
5. Click **Save**.
6. Reboot the device.

The **IGEL Advanced Device Redirection USB app** (additional license required) also includes controls for USB devices.
Learn more: IGEL Advanced Device Redirection USB[38]

36. https://kb.igel.com/en/igel-os/11.10.270/when-to-use-usb-redirection
37. https://kb.igel.com/en/igel-os-base-system/current/usb-access-control-in-igel-os-12
38. https://kb.igel.com/en/igel-apps/current/igel-advanced-device-redirection-usb

Disabling USB Boot

Rationale

Disabling USB boot prevents the device from booting another operating system, which could otherwise be used to manipulate or overwrite IGEL OS on the internal storage, whether intentionally or accidentally.

Instructions for IGEL Devices

USB boot is **disabled by default** in factory settings on IGEL UD LX devices.

If it has been enabled and you want to disable it again, follow these steps:

1. Hold down the [Del] key ([F2] for UD2 devices) while the system is booting.
   The UEFI menu opens.
2. Use the arrow and return keys to navigate to **SCU**.
3. If prompted, enter the **UEFI password** (if one is set).
   The Setup Utility opens.
4. Go to the **Boot** section.
5. Set **USB Boot** to **Disabled**.
6. Press [F10] to save and exit.
7. Confirm **Exit Saving Changes?** when prompted.
   The device will reboot.

⚠ Set a **UEFI Password** to prevent unauthorized users from re-enabling USB boot or altering boot settings.

Instructions for 3rd-Party Devices Converted with OSC

→ Refer to the BIOS/UEFI vendor documentation for your hardware.

ℹ Alternatively, you can try the following keys to access the BIOS/UEFI setup during boot:

- [F12] (common)
- [F10] (Intel devices)
- [F9] (Hewlett-Packard devices)
- [Del], [F1], or [F2] (for other systems)

Configuring Remote Access and Management

Remote management via the Universal Management Suite (UMS) and remote access are powerful features of IGEL OS.
To maintain system integrity, always select secure settings and disable all remote features you do not actively use.

Tying Endpoints to Your UMS instance

Rationale

Devices that have remote management enabled but are not yet tied to a UMS instance can be taken over by an attacker's UMS. To prevent unauthorized management, ensure that all IGEL devices on your network are registered with your organization's UMS.

Instructions

There are several ways to register devices on UMS 12:

- Scanning the local network for devices
  --> See: How to Scan the Network for Devices and Register Them[39]
- Using automatic registration in a local network (DHCP or DNS)
  --> See: Registering Devices Automatically on the IGEL UMS[40]
- Importing devices from a CSV File
  --> See: Importing Devices[41]
- Onboarding devices via IGEL Onboarding Service (OBS)
  This method supports remote devices outside the corporate network, such as those used by home office or mobile users.
  --> See: Initial Configuration of the IGEL Onboarding Service[42]

39. https://kb.igel.com/en/universal-management-suite/current/how-to-scan-the-network-for-devices-and-register-d
40. https://kb.igel.com/en/universal-management-suite/current/registering-devices-automatically-on-the-igel-ums
41. https://kb.igel.com/en/universal-management-suite/current/importing-devices
42. https://kb.igel.com/en/how-to-start-with-igel/current/initial-configuration-of-the-igel-onboarding-servi

Using Secure Shadowing

Rationale

If you intend to use shadowing (viewing or controlling a user's desktop remotely) on IGEL OS 12, several configuration options can improve both security and privacy.

Instructions

By default, Shadowing in IGEL OS 12 uses TLS and certificate-based authentication. These mechanisms provide encryption and verification of the shadowing connection.

You can disable **Deny shadowing via external VNC tool** to allow the use of third-party VNC clients, however, this is not recommended, as doing so may result in unencrypted VNC traffic.

To configure secure shadowing:

1. In IGEL Setup, go to **System > Remote Access > Shadow**.
2. Activate **Allow Remote Shadowing**.
3. Configure as many of the following options as applicable to your use case. Each additional setting improves security and, in most cases, enhances user privacy:
    - Enable **Use Password** and set a strong password (not required in default TLS mode).
        - Maximum length for this password: 8 characters**.**
    - Enable **Prompt User to allow Remote Session**.
    - Enable **Allow User to disconnect Remote Shadowing**.
    - Disable **Allow Input from Remote**.
4. Click **Save**.

In the **UMS Console**, you can also enable shadowing session logging under:
UMS Administration > Global Configuration > Remote Access
This records which users have performed shadowing, providing an audit trail for security reviews.

Disabling Secure Terminal

Rationale

The Secure Terminal server on IGEL OS is a network service providing a TLS/SSL-encrypted Telnet session.
This service is not required for normal IGEL OS 12 management, which is handled via the Universal Management Suite (UMS).
Disabling it reduces the number of active network services and therefore decreases the system's attack surface.

Instructions

By default, the Secure Terminal is not active. If you want to deactivate it at any time, follow these steps:

1. In IGEL Setup, go to **System > Remote Access > Secure Terminal**.
2. Deactivate **Secure Terminal**.
3. Click **Save**.

> In the **UMS Console**, you can enable logging of users who have accessed the Secure Terminal:
> **UMS Administration > Global Configuration > Remote Access**.

Using SSH Securely

An **OpenSSH server** is included in the IGEL OS 12 base system but is not running by default.
SSH is not required for normal device management, which is handled via the Universal Management Suite (UMS).
However, SSH can be useful for debugging or automation tasks, such as running interactive sessions or executing commands remotely.

Instructions

1. In IGEL Setup, go to **System > Remote Access > SSH**.
2. Activate **Enable** to start the SSH server.
3. Leave **Permit empty passwords** deactivated.
4. Leave **Permit administrator login** deactivated.
5. Allow **User Access** for the user, who can execute commands with standard (non-administrative) privileges.
6. Deny **User Access** for ruser.
7. Leave **Permit X11 forwarding** deactivated.
8. (Optional) Under **Hosts**, specify a comma-separated list of allowed DNS names or IP addresses.
   You can also leave the asterisk (`*`) to allow all hosts (not recommended for secure environments).
9. Click **Save**.

Using Public Key Authentication

Public key authentication for SSH is more secure than using passwords. It relies on cryptographic key pairs instead of credentials transmitted over the network, significantly reducing the risk of brute-force or credential theft attacks.

1. (Optional) If you do not already have an SSH key pair, create one on your remote host using the `ssh-keygen` command.
   --> For details on available options, see: ssh-keygen manual page[43]
2. Make a copy of your **public SSH key** in another directory and name the file `authorized_keys`.
3. Create a new **File Object** in the **UMS**:
   a. Upload the `authorized_keys` file.
   b. Set **Classification** to **Undefined**.
   c. Set **Device file location** to `/userhome/.ssh/`
   d. Set **Owner** to **User**.
   e. Set **Owner access rights** to **rwx**.
   f. Set **Other access rights** to **(None)**.

43. https://man.openbsd.org/ssh-keygen

Wi-Fi and Bluetooth

Rogue or unencrypted Wi-Fi access points can put your data at risk, as can insecure Bluetooth connections. If your device includes Wi-Fi or **Bluetooth** functionality, ensure that these interfaces are securely configured or disabled entirely when not required.

Restricting Wi-Fi Access

Rationale

Using an unencrypted Wi-Fi network or connecting to a rogue access point exposes user data to interception and compromise.
Enable strong encryption (e.g., WPA2/WPA3) and restrict Wi-Fi access to a predefined, trusted network.

Instructions

By default, an IGEL OS 12 user can select any available Wi-Fi network via the Wi-Fi tray icon.
If this behavior is not desired, you can remove the tray icon and allow the device to connect automatically only to one specific network:

1. In IGEL Setup, go to **User Interface > Desktop > Taskbar Items.**
2. Deactivate **Show Wi-Fi connection status tray icon on desktop**.
3. In IGEL Setup, go to **Network > Wireless > Wi-Fi Networks**.
4. Create the desired Wi-Fi network and activate **Enable automatically connect** for it.

The device will now automatically connect to the configured network upon user login.
If multiple Wi-Fi networks are configured, the device will connect to the **first network** in the list with **Enable automatically connect** activated.

Bluetooth

Rationale

If your device has a Bluetooth interface, it may be used to access or transfer data. Disabling the interface reduces the risk of data theft or unauthorized access.

Instructions

By default, Bluetooth is deactivated on IGEL OS. If you want to disable it at any time, follow these steps:

1. In IGEL Setup, go to **Devices > Bluetooth**.
2. Deactivate **Bluetooth**.
3. Click **Save**.

Network Security

Service Minimalism

Run as few network services on IGEL OS 12 as possible. Once an OS 12 endpoint is registered with your UMS, it exposes only a single service — the portmapper. Even that service may not be required and can be deactivated.
--> See: Disabling RPC Portmapper Service[44]

Host-based Firewall with iptables

By default, no host-based firewall is active on IGEL OS 12. If you follow the Service Minimalism principle, you may not need one.

However, the Linux kernel included in IGEL OS 12 supports comprehensive firewall functionality that can be configured using the `iptables` or `nftables` command-line tools. You can deploy firewall rules to endpoints by configuring commands in:
System > System Customization > Custom Commands Base > Network > Initialization within a UMS Profile.

44. https://kb.igel.com/en/security-safety/current/disabling-rpc-portmapper-service

Using IGEL UD Pocket for BYOD Devices

Rationale

Allowing users to access company resources with their own devices and operating systems introduces security risks. Such systems may have insecure configurations or contain malware. Additionally, company data should never be stored on users' private devices.

Instructions

Use the IGEL UD Pocket to enable secure access from personal (BYOD) devices. This ensures that users operate within a trusted and controlled IGEL OS environment.
Because the UD Pocket does not access the device's internal mass storage, corporate data and personal data remain separated.

For more details on the IGEL UD Pocket and how to select it during the boot process, see: How to Use IGEL OS 12 with UD Pocket[45].

45. https://kb.igel.com/en/igel-os-base-system/current/how-to-use-igel-os-12-with-ud-pocket

Product Security Archive

UMS TLS Support
Notice from 2018-05-12
Since version 5.08.100, the UMS support TLS v1.2 only.

Deprecation of Weak Algorithms
Notice from 2018-03-13
See *IGEL OS 11.10 > IGEL OS Articles > SSH > Current:SSH: Deprecation of Weak Algorithms as of IGEL Linux 10.04.100*

IGEL Meltdown and Spectre (2)
Notice from 2018-02-01
Security fixes available for download[46]
See newsletter[47]

IGEL Meltdown and Spectre
Notice from 2018-01-18
Security fixes available for download[48]
See newsletter[49]

KRACK Attacks
Notice from 2017-10-23
Security fixes available for download[50]
See newsletter[51]

46. https://www.igel.com/software-downloads/
47. https://mailchi.mp/6ede7858d1c2/igel-technical-newsletter-january18_meltdown_spectre-1289945
48. https://www.igel.com/software-downloads/
49. http://mailchi.mp/6d07867522c2/igel-technical-newsletter-january18_meltdown_spectre-1289889
50. https://www.igel.com/software-downloads/
51. http://mailchi.mp/b68f2468dce3/igel-technical-newsletter-august-1289593

Reporting Vulnerabilities in IGEL Products

Are you a security researcher who has discovered a vulnerability in an IGEL product? Please contact security@igel.com[52] to report it. A PGP/GPG key for confidential communication is available upon request.

IGEL customers are asked, however, to open a case on the IGEL Customer Portal[53].

52. mailto:security@igel.com
53. https://support.igel.com/

UEFI Secure Boot Enabling Guides

As of IGEL OS 10.04.100, and as of Microsoft Windows 10 IoT 4.03.100, UEFI Secure Boot has been introduced to IGEL devices.

For the devices listed below, activation of UEFI Secure Boot may be needed first; for instructions, click the appropriate link:

- UD2-LX 40 (see page 224)
- UD3-LX 50 (see page 232)
- UD3-LX 51 (see page 239)
- UD6-LX 51 (see page 247)
- UD7-LX 10 (see page 255)

- UD3-W10 51 (see page 261)
- UD6-W10 51 (see page 268)
- UD7-W10 10 (see page 276)

IGEL OS

Enabling UEFI Secure Boot in UD2-LX 40

Prerequisites

- IGEL OS 10.04.100 or higher
- BIOS BayTrail.5.04.32.0022 or higher

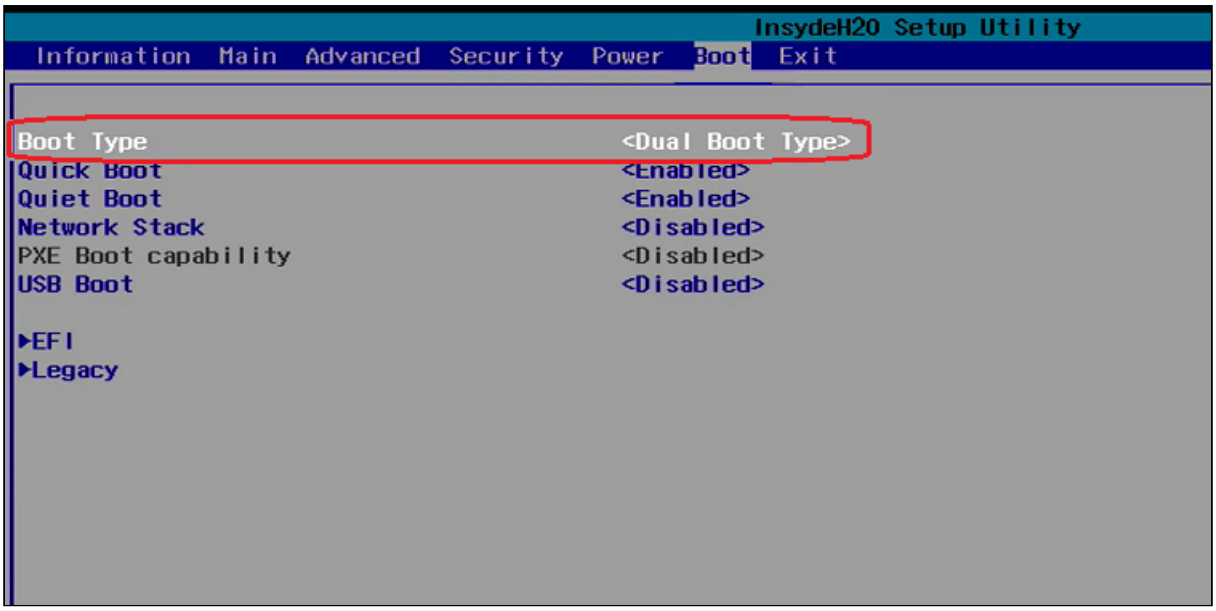
To check the BIOS version, open the InsydeH20 Setup Utility as described below (step 3). Press [F9] to open the **System Information** window. In the **System Information** window, check that the BIOS version corresponds to *BayTrail.5.04.32.0022* or higher. For more information, see *Hardware > Versions of Hardware > (1-en) Hardware > (1-en) Hardware FAQs > (1-en) How Can I Update the BIOS Version?*

It is crucial to set a BIOS password to prevent users from disabling Secure Boot.

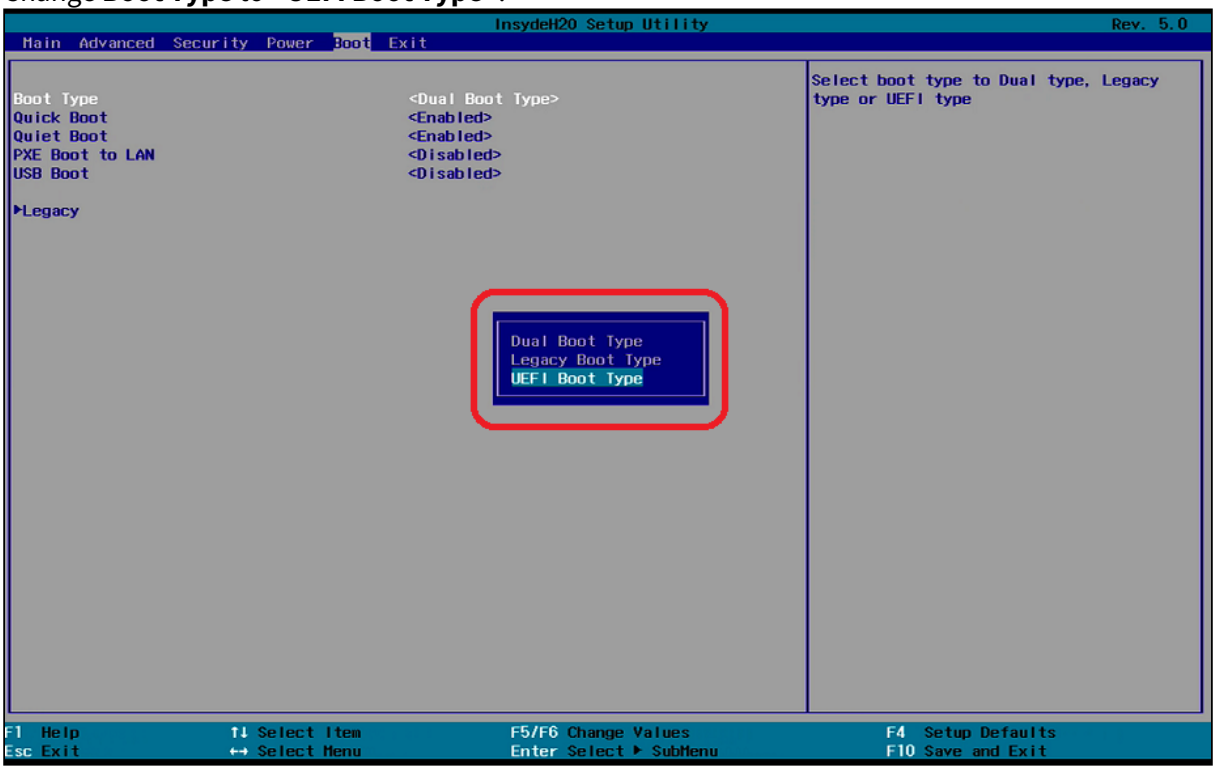
Changing the Device's Boot Type to UEFI Boot

1. Turn on (or restart) the IGEL device.
2. During boot, hold the [F2] key until you see the menu shown below.
3. Using the arrow keys, move to the option **SCU** and press [ENTER]. This will open the InsydeH20 Setup Utility.

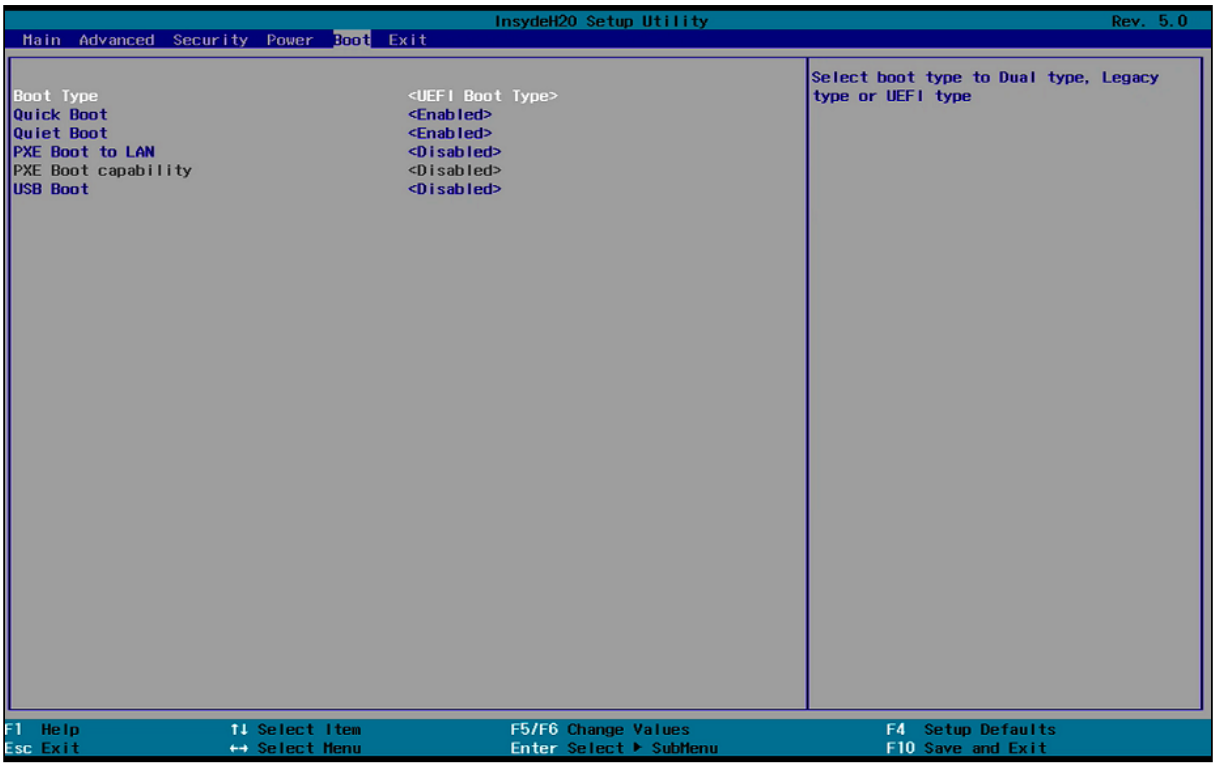
4. Using the arrow keys, move to the **Boot** tab. Ýou will find **Boot Type** set to **<Dual Boot Type>**.



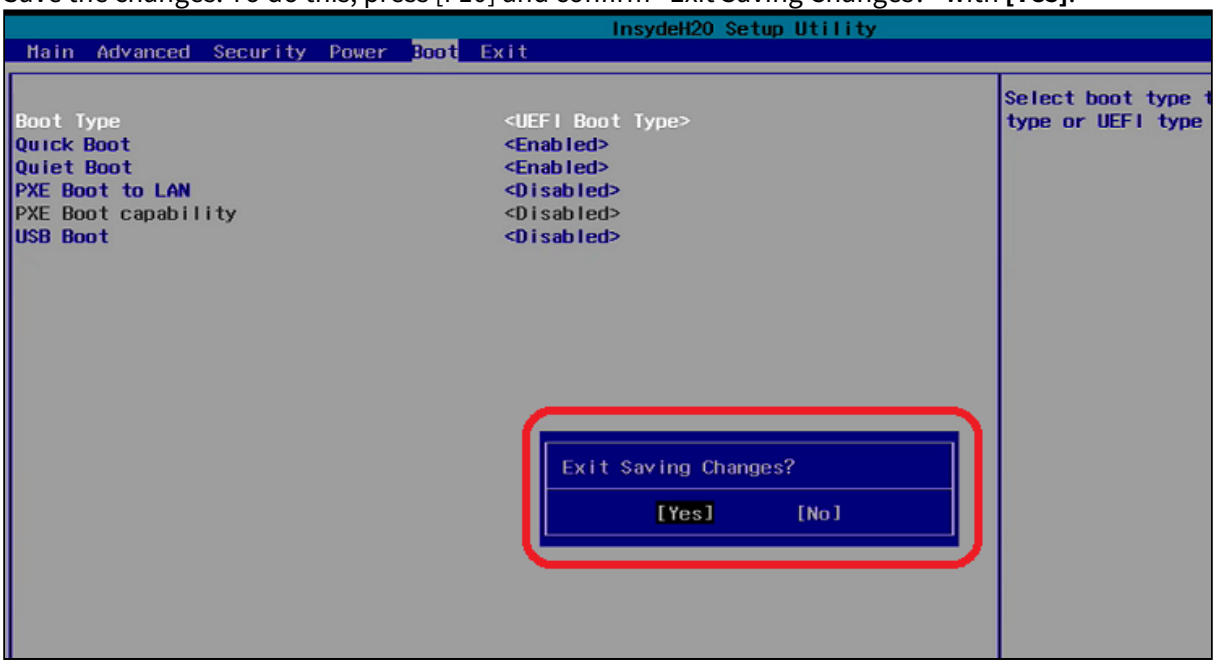
5. Change **Boot Type** to **<UEFI Boot Type>**.



Boot Type is now set to **<UEFI Boot Type>**.



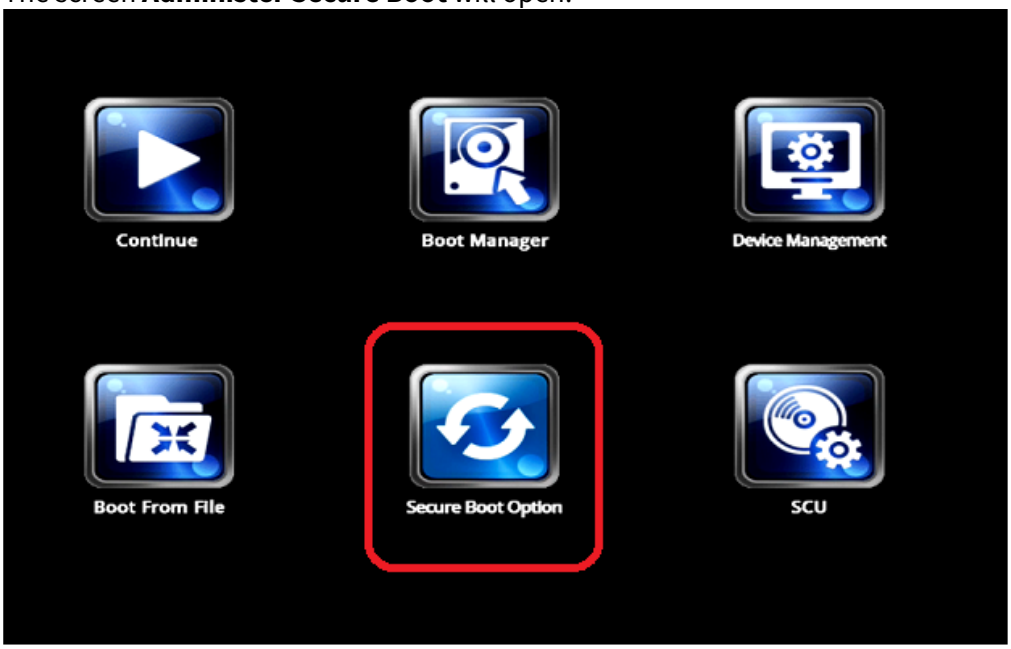
6. Save the changes. To do this, press [F10] and confirm "Exit Saving Changes?" with **[Yes]**.



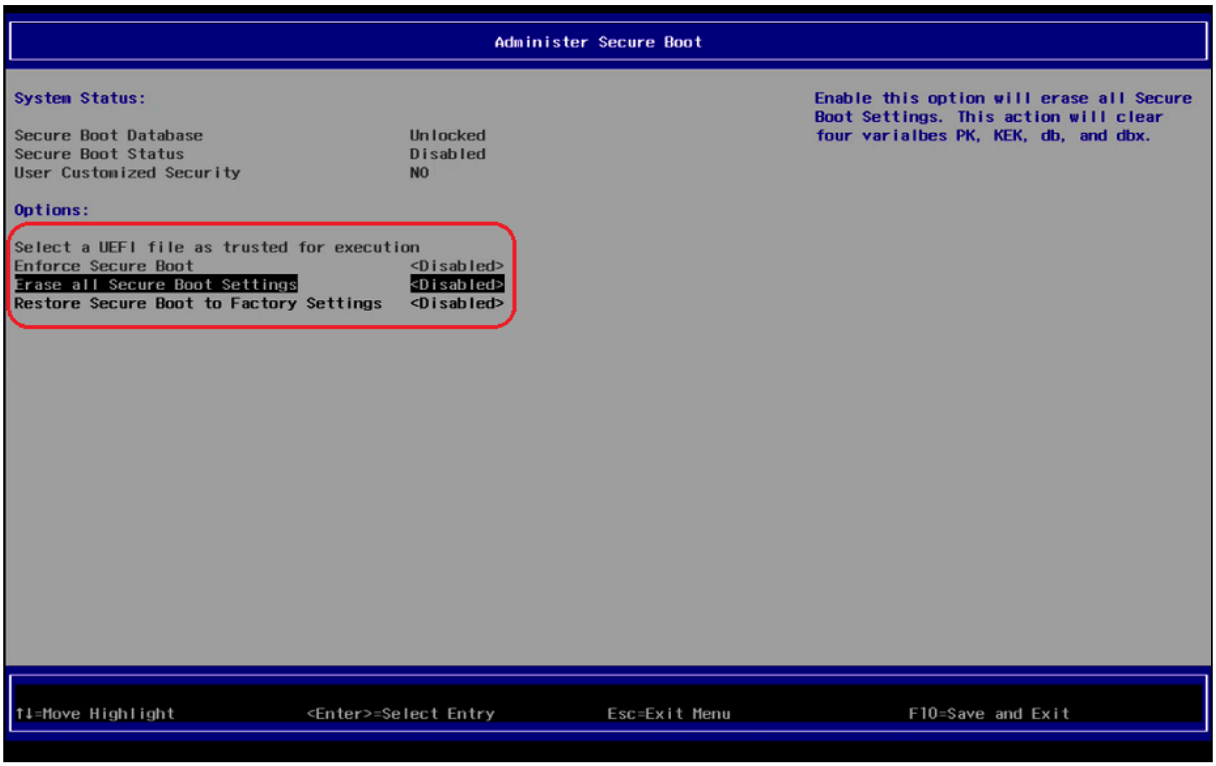
The settings are now saved and the device is rebooted.

Activating the Secure Boot Feature

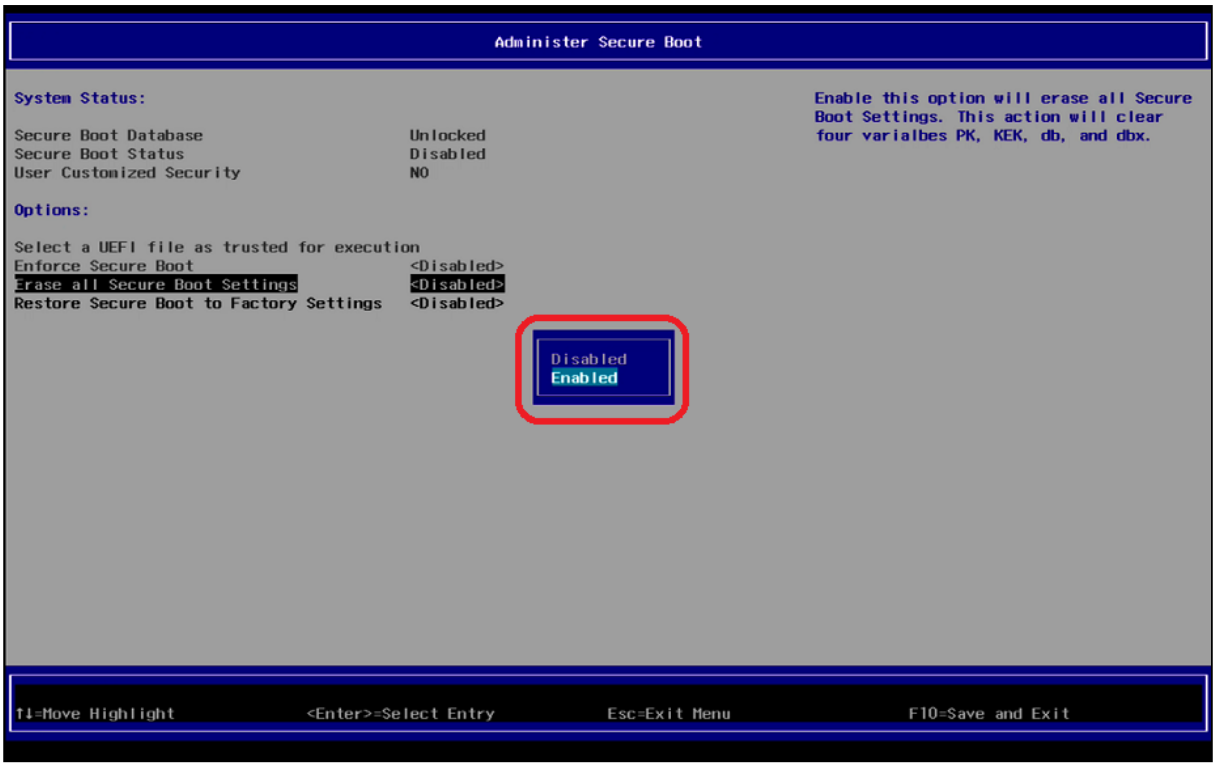
1. Turn on (or restart) the IGEL device.
2. During boot, hold the [F2] key until you see the menu shown below.
3. Using the arrow keys, navigate to the option **Secure Boot Option** and press [ENTER].
   The screen **Administer Secure Boot** will open.



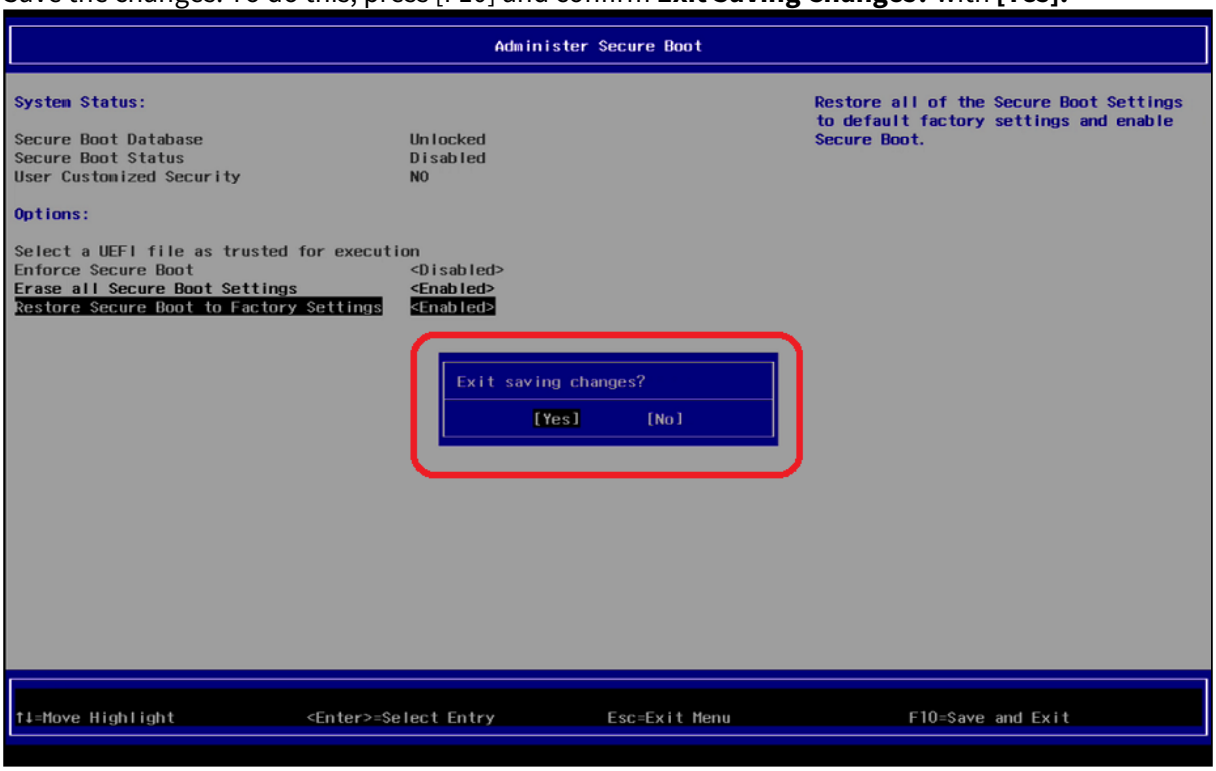
4. In the screen **Administer Secure Boot**, you will find **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** set to **<Disabled>**.



5. Change **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** to **<Enabled>**.
   If **"Enforce Secure Boot"** is not grayed out as in the picture below, change that option to as well.



6. Save the changes. To do this, press [F10] and confirm **Exit Saving Changes?** with **[Yes].**



The changes are now saved and the device is rebooted.

7. As a last step, verify that Secure Boot is working, see Verifying that Secure Boot is Enabled (see page 280).

Enabling UEFI Secure Boot in UD2-LX 50/51

UEFI Secure Boot is already a default setting in UD2-LX 50 and UD2-LX 51.

If you have disabled secure boot, you will need to reverse the settings you made.

Enabling UEFI Secure Boot in UD3-LX 50

Prerequisites

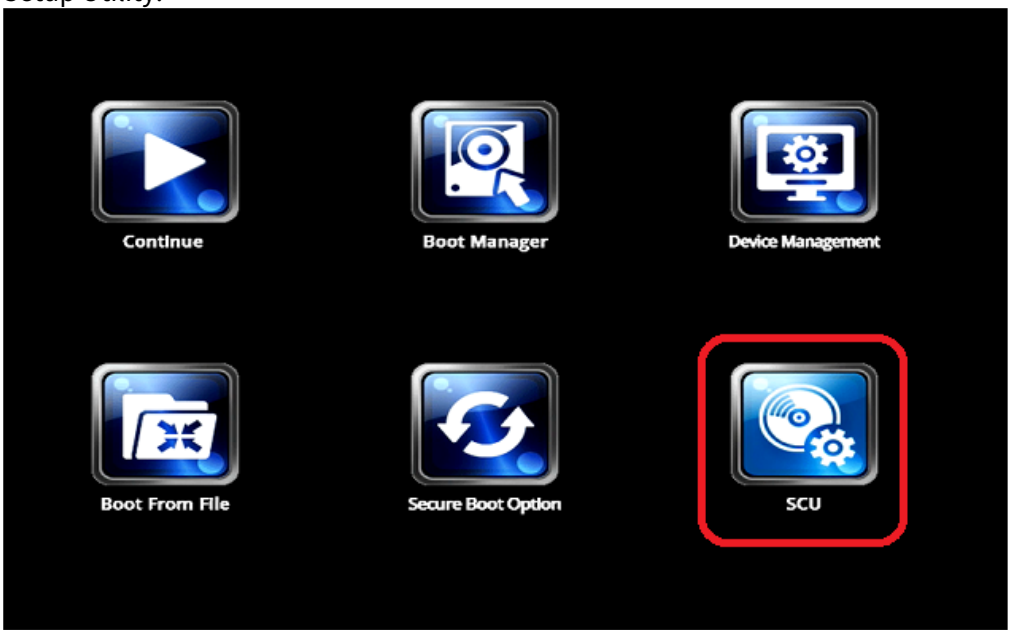
- IGEL OS 10.04.100 or higher
- BIOS version 3.A. 13-11202017 or higher

To check the BIOS version, open the InsydeH20 Setup Utility as described below (step 3). Press [F9] to open the **System Information** window. In the **System Information** window, check that the BIOS version corresponds to *3.A. 13-11202017* or higher. For more information, see *Hardware* > *Versions of Hardware* > *(1-en) Hardware* > *(1-en) Hardware FAQs* > *(1-en) How Can I Update the BIOS Version?*.

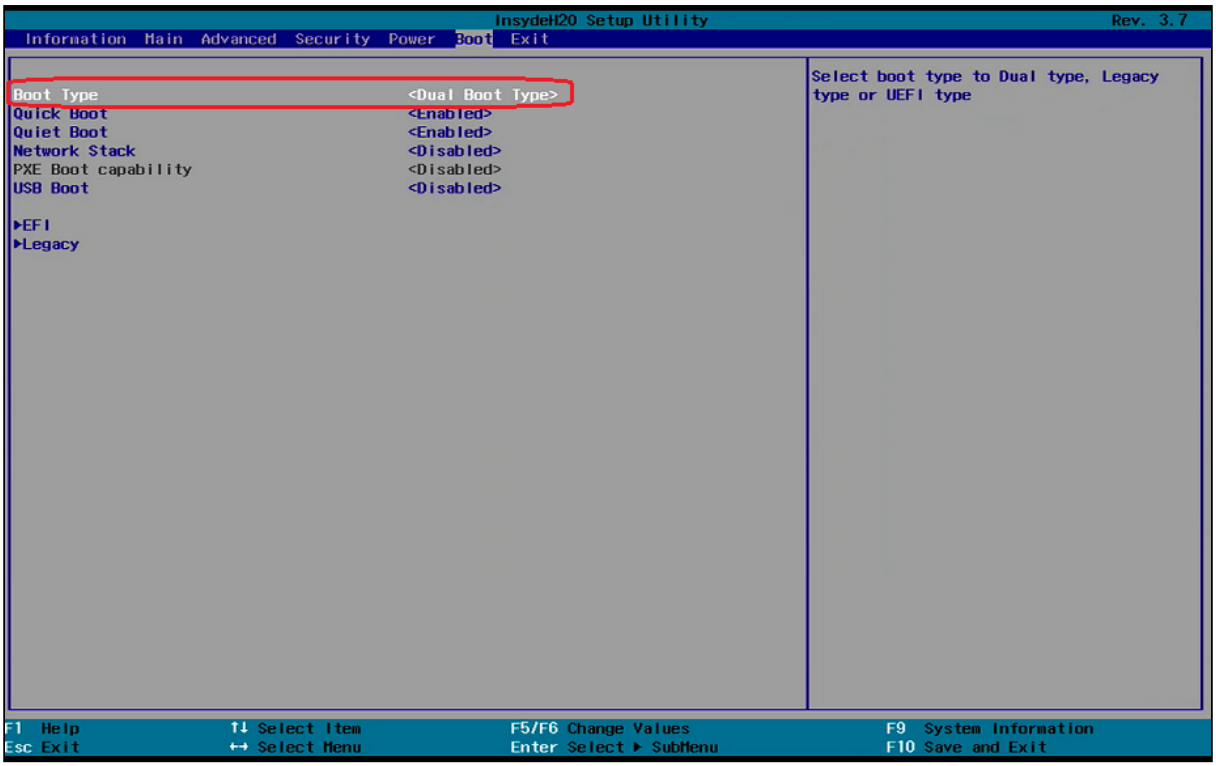
It is crucial to set a BIOS password to prevent users from disabling Secure Boot.

Changing the Device's Boot Type to UEFI Boot

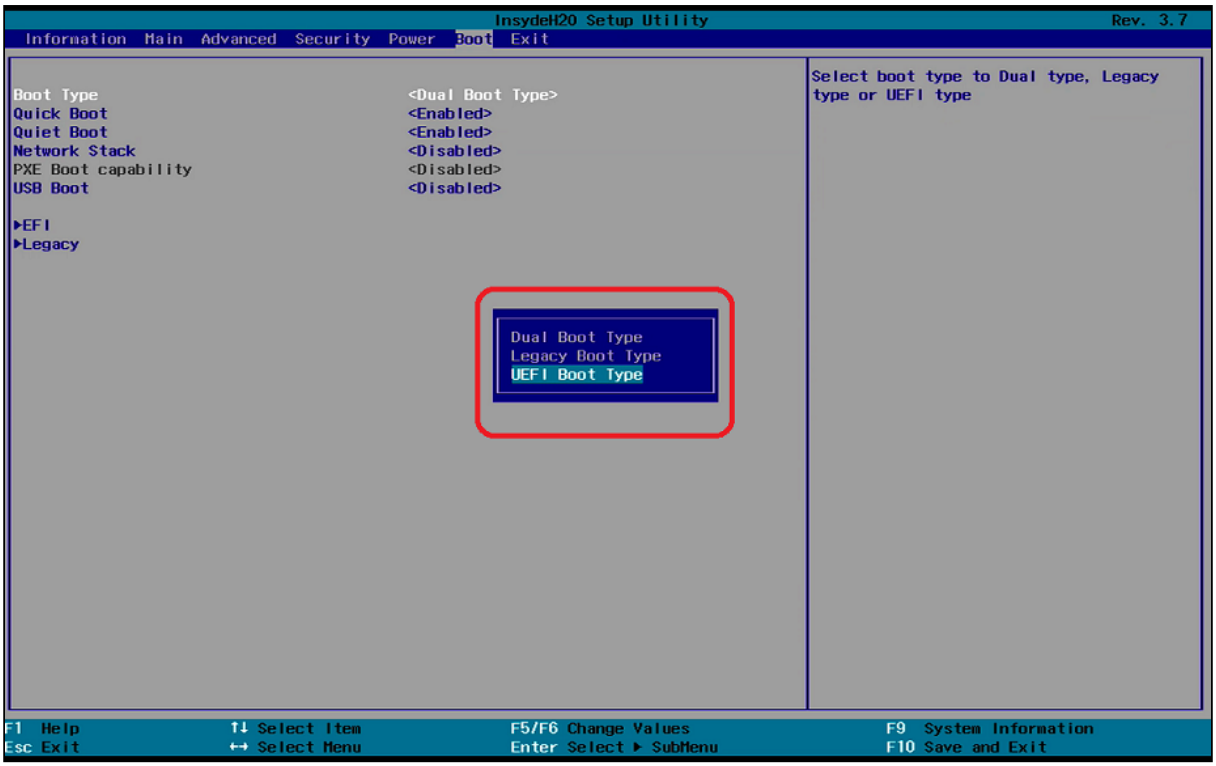
1. Turn on (or restart) the IGEL device.
2. During boot, hold the [DEL] key until you see the menu shown below.
3. Using the arrow keys, navigate to the option **SCU** and press [ENTER]. This will open the InsydeH20 Setup Utility.



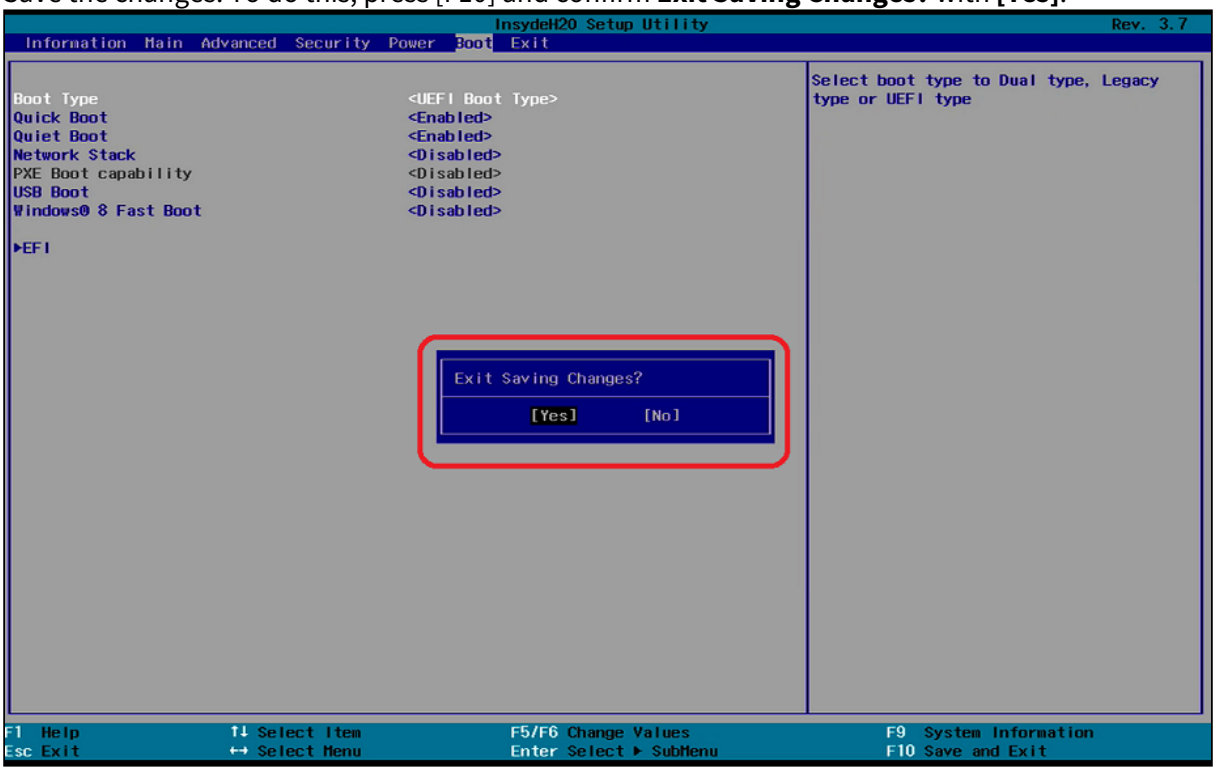
4. Using the arrow keys, move to the tab **Boot**. You will find **Boot Type** set to **<Dual Boot Type>**.



5. Change **Boot Type** to **<UEFI Boot Type>**.



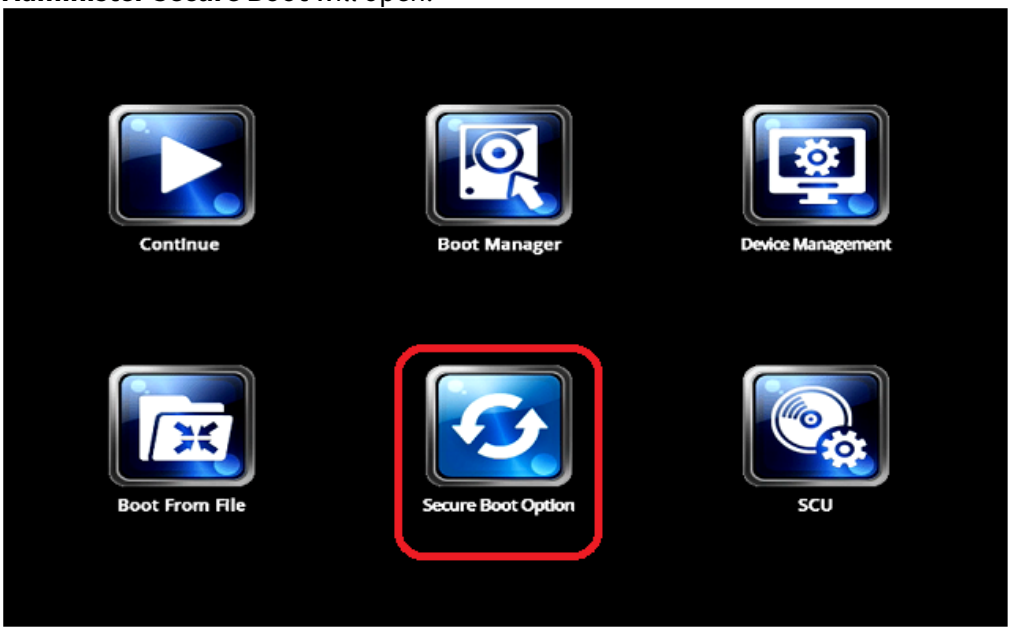
6. Save the changes. To do this, press [F10] and confirm **Exit Saving Changes?** with **[Yes]**.



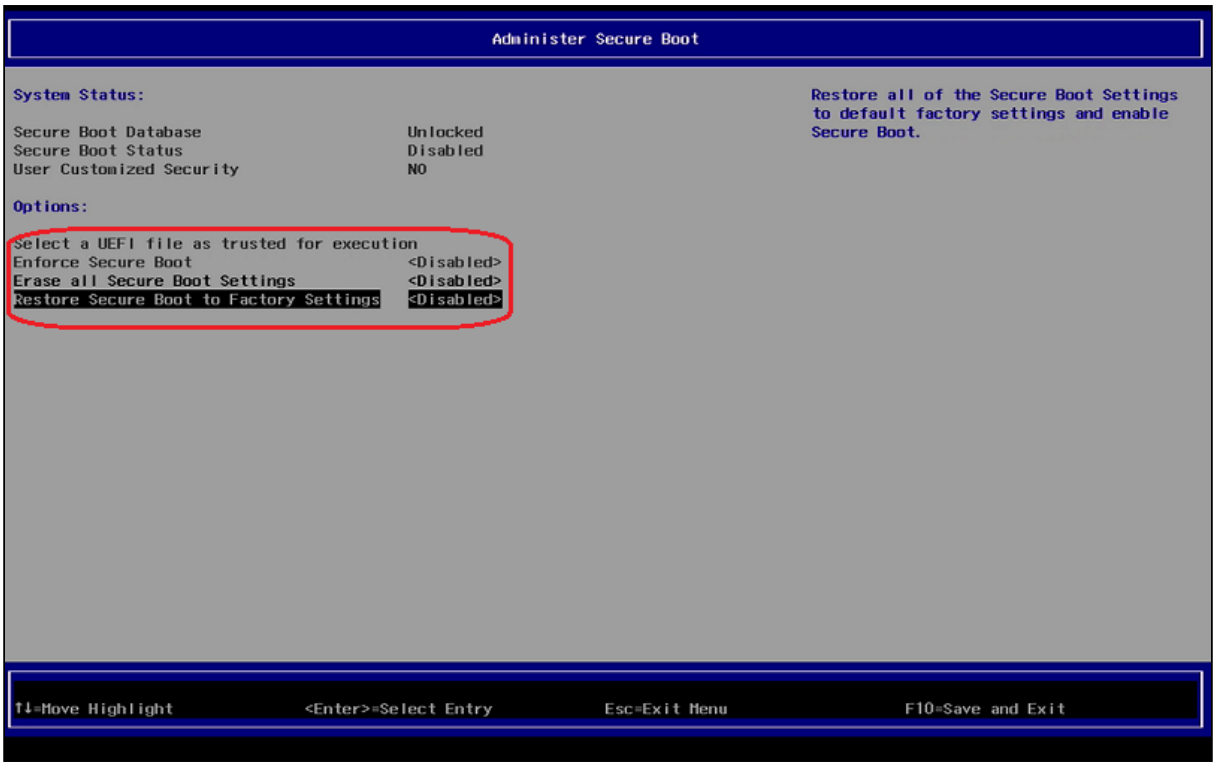
The changes will be saved and the device will be rebooted.

Activating the Secure Boot Feature

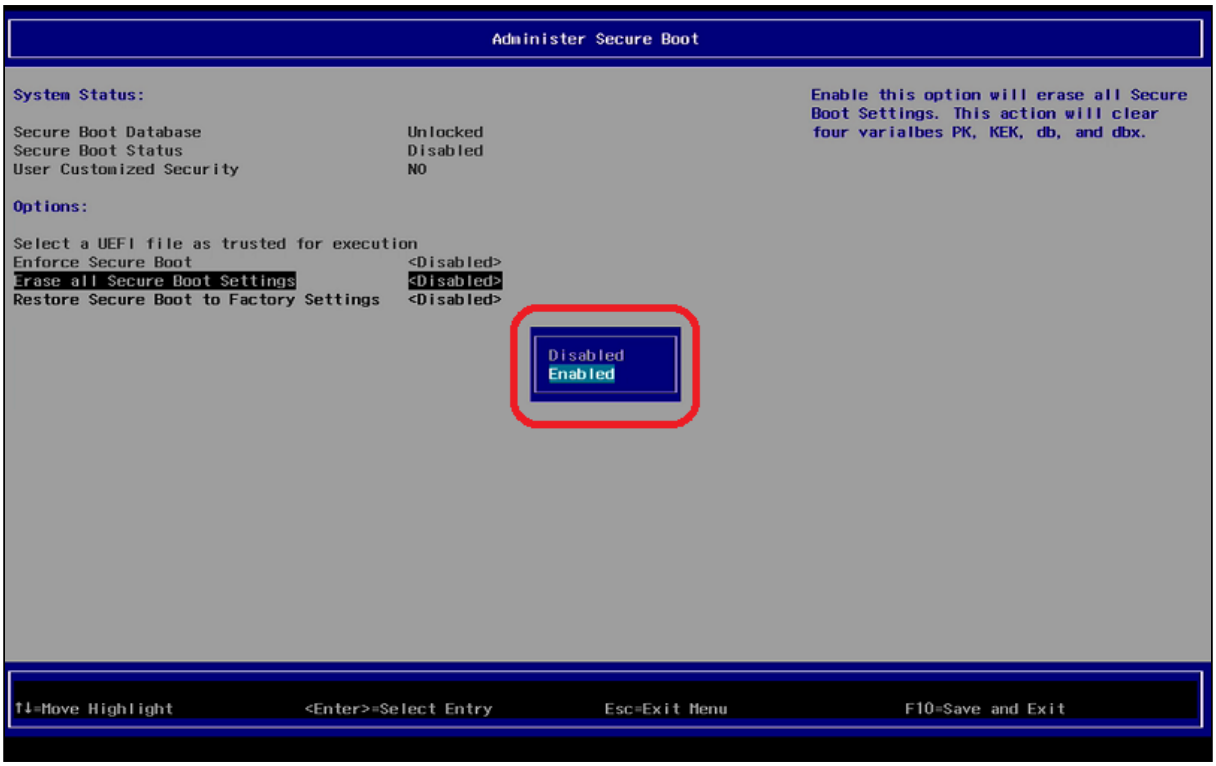
1. Turn on (or restart) the IGEL device.
2. Using the arrow keys, move to **Secure Boot Option** and press [ENTER]. The BIOS screen **Administer Secure Boot** will open.



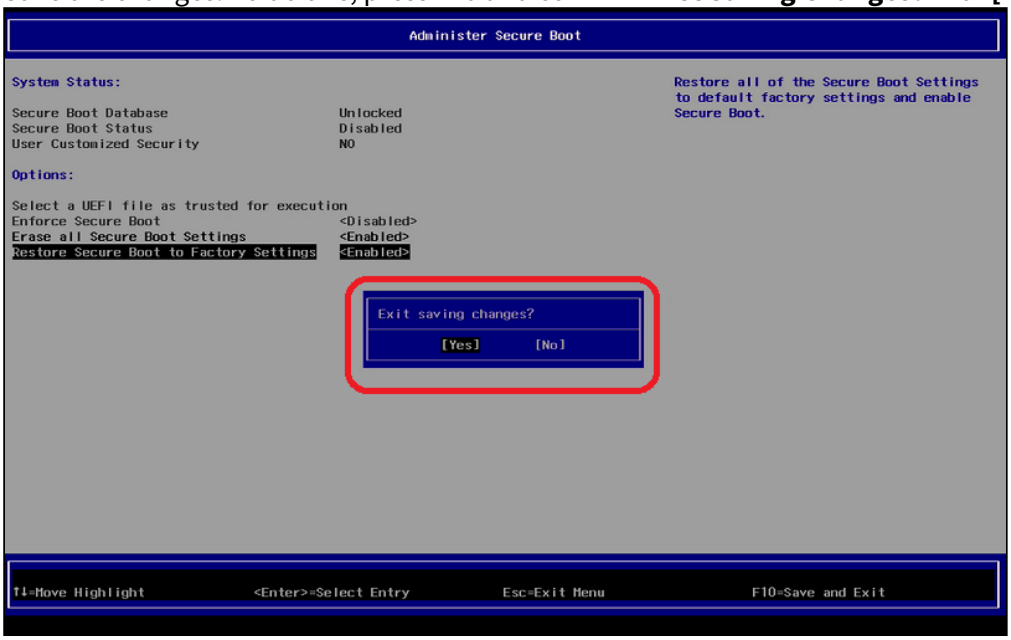
3. In the screen **Administer Secure Boot**, you will find **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** set to **<Disabled>**.



4. Change **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** to **<Enabled>**.
   If **"Enforce Secure Boot"** is not grayed out as in the picture below, change that option to as well.



5. Save the changes. To do this, press F10 and confirm **Exist Saving Changes?** with **[Yes]**.



The changes will be saved and the device will be rebooted.

6. As a last step, verify that Secure Boot is working, see Verifying that Secure Boot is Enabled (see page 280).

Enabling UEFI Secure Boot in UD3-LX 51

Prerequisites

- IGEL OS 10.04.100 or higher
- BIOS version 3.A. 13-11202017 or higher

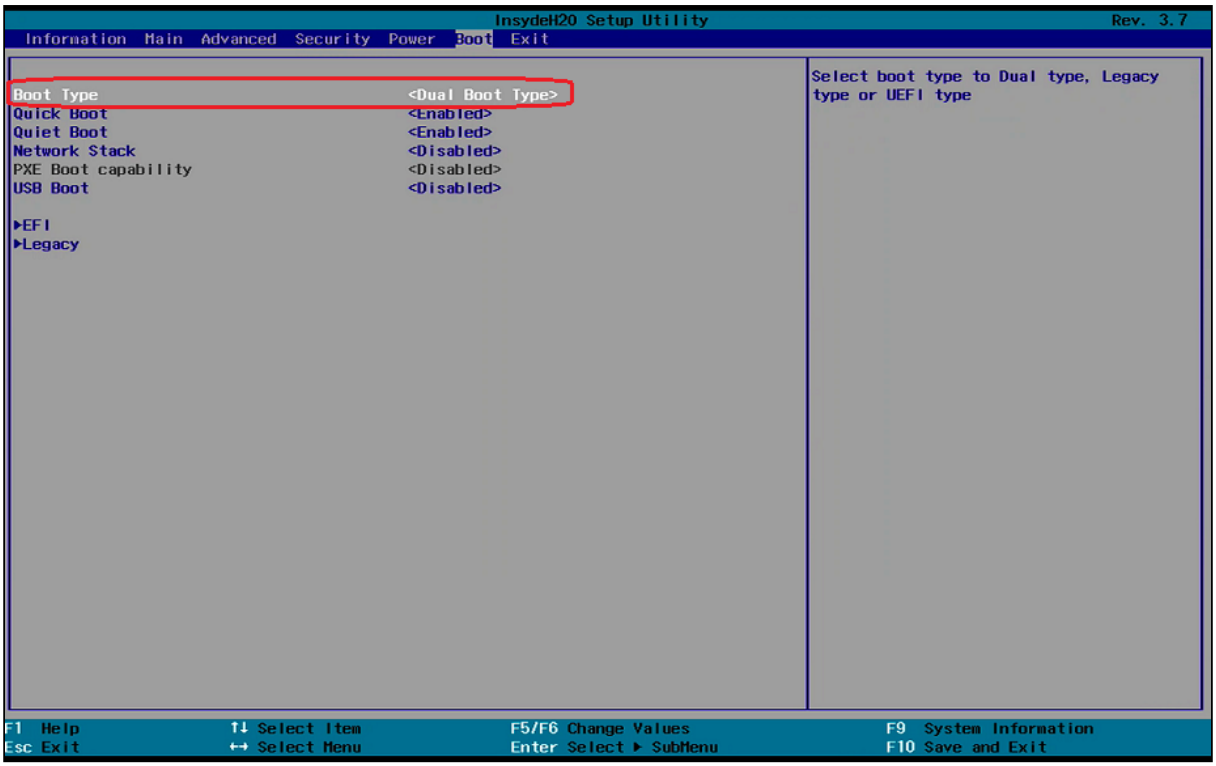
To check the BIOS version, open the InsydeH20 Setup Utility as described below (step 3). Press [F9] to open the **System Information** window. In the **System Information** window, check that the BIOS version corresponds to *3.A. 13-11202017* or higher. For more information, see *Hardware* > *Versions of Hardware* > *(1-en) Hardware* > *(1-en) Hardware FAQs* > *(1-en) How Can I Update the BIOS Version?*.

It is crucial to set a BIOS password to prevent users from disabling Secure Boot.

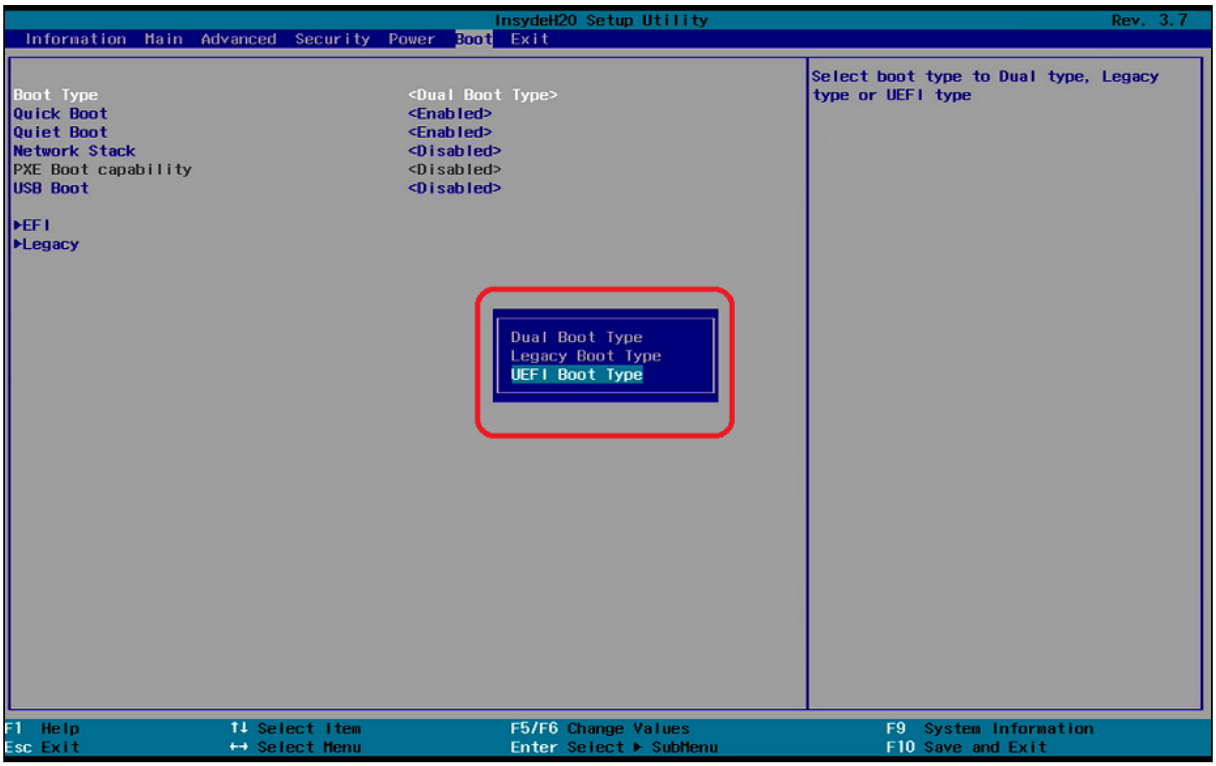
Changing the Device's Boot Type to UEFI Boot

1. Turn on (or restart) the IGEL device.
2. During boot, hold the [DEL] key until you see the menu shown below.
3. Using the arrow keys, navigate to the option **SCU** and press [ENTER]. This will open the InsydeH20 Setup Utility.

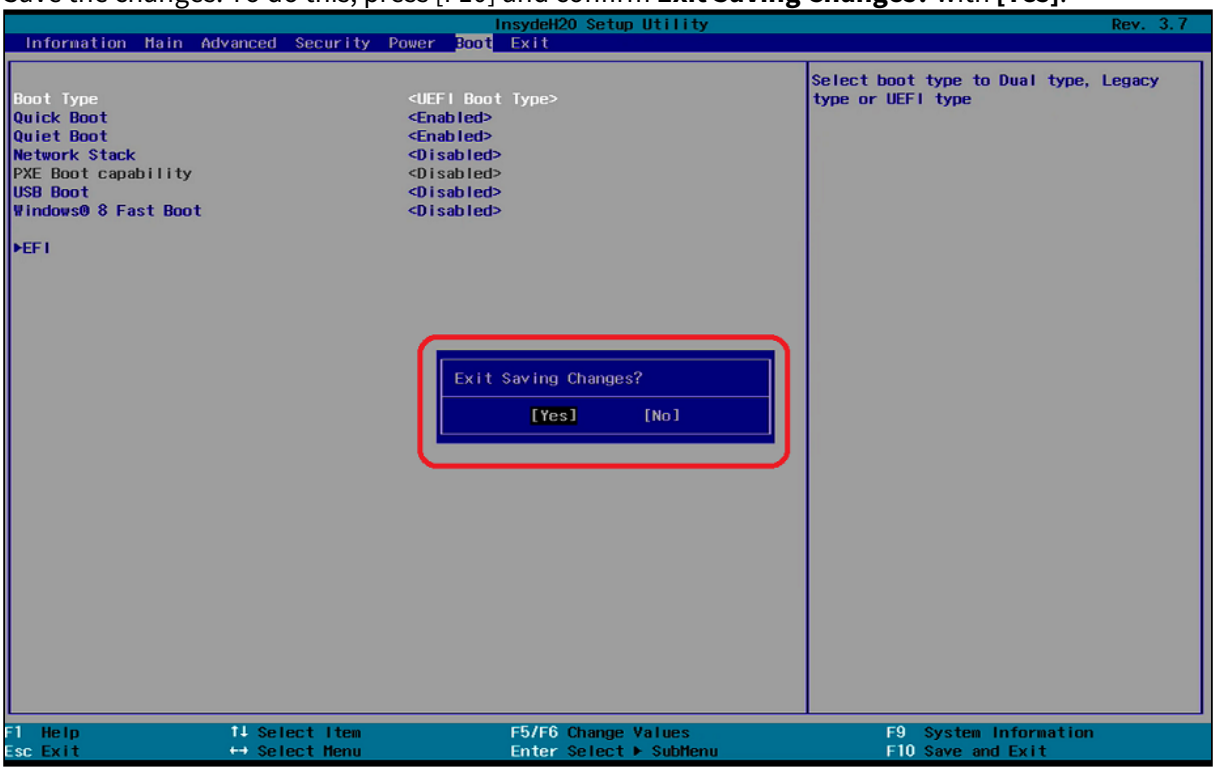
4. Using the arrow keys, move to the tab **Boot**. You will find **Boot Type** set to **<Dual Boot Type>**.



5. Change **Boot Type** to **<UEFI Boot Type>**.



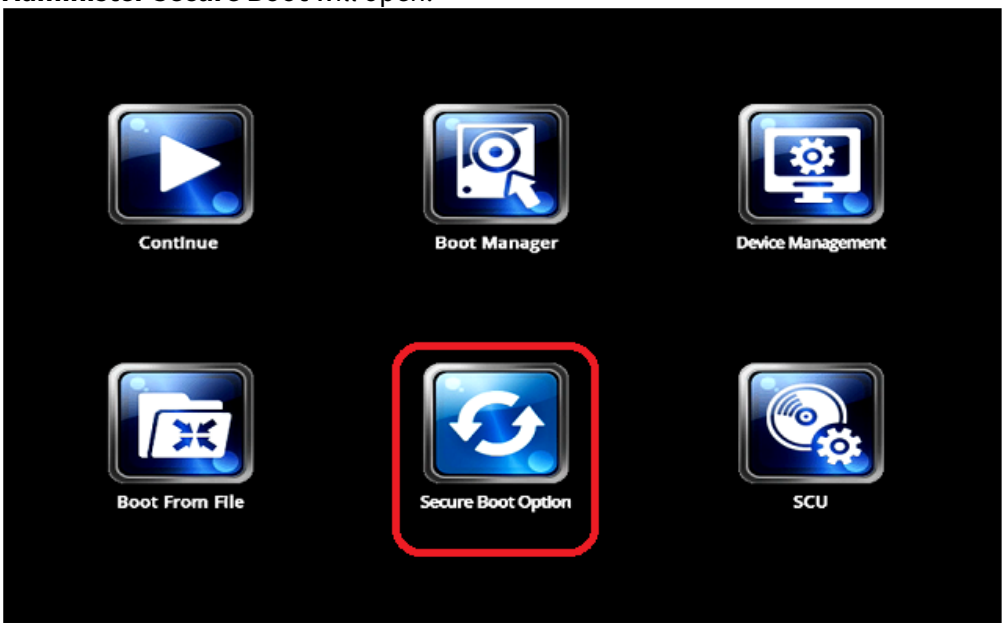
6. Save the changes. To do this, press [F10] and confirm **Exit Saving Changes?** with **[Yes]**.



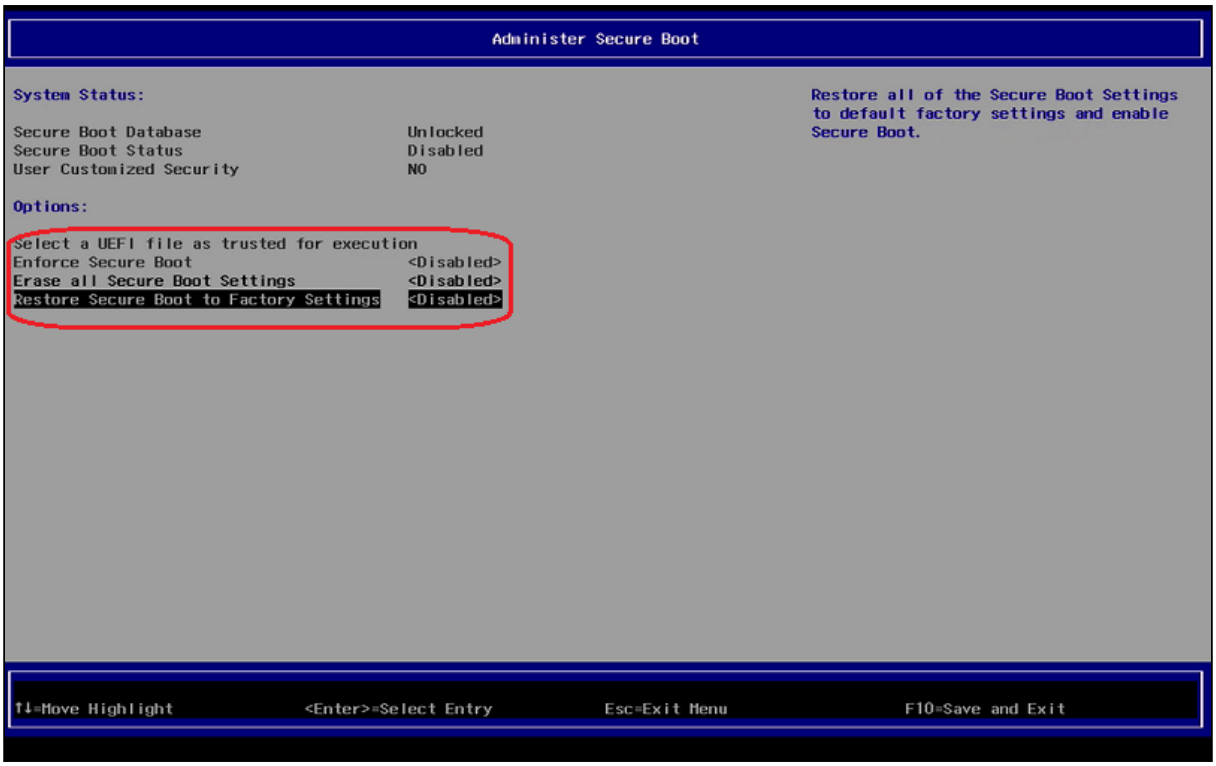
The changes will be saved and the device will be rebooted.

Activating the Secure Boot Feature

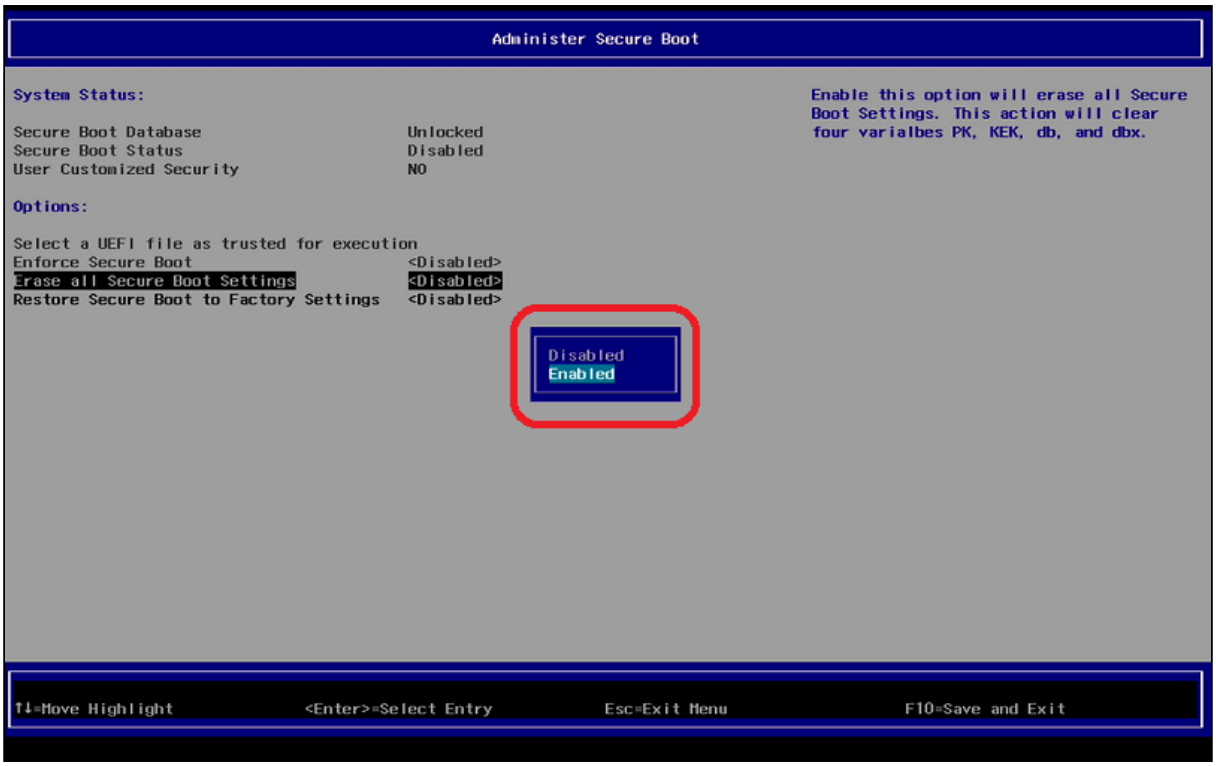
1. Turn on (or restart) the IGEL device.
2. Using the arrow keys, move to **Secure Boot Option** and press [ENTER]. The BIOS screen **Administer Secure Boot** will open.



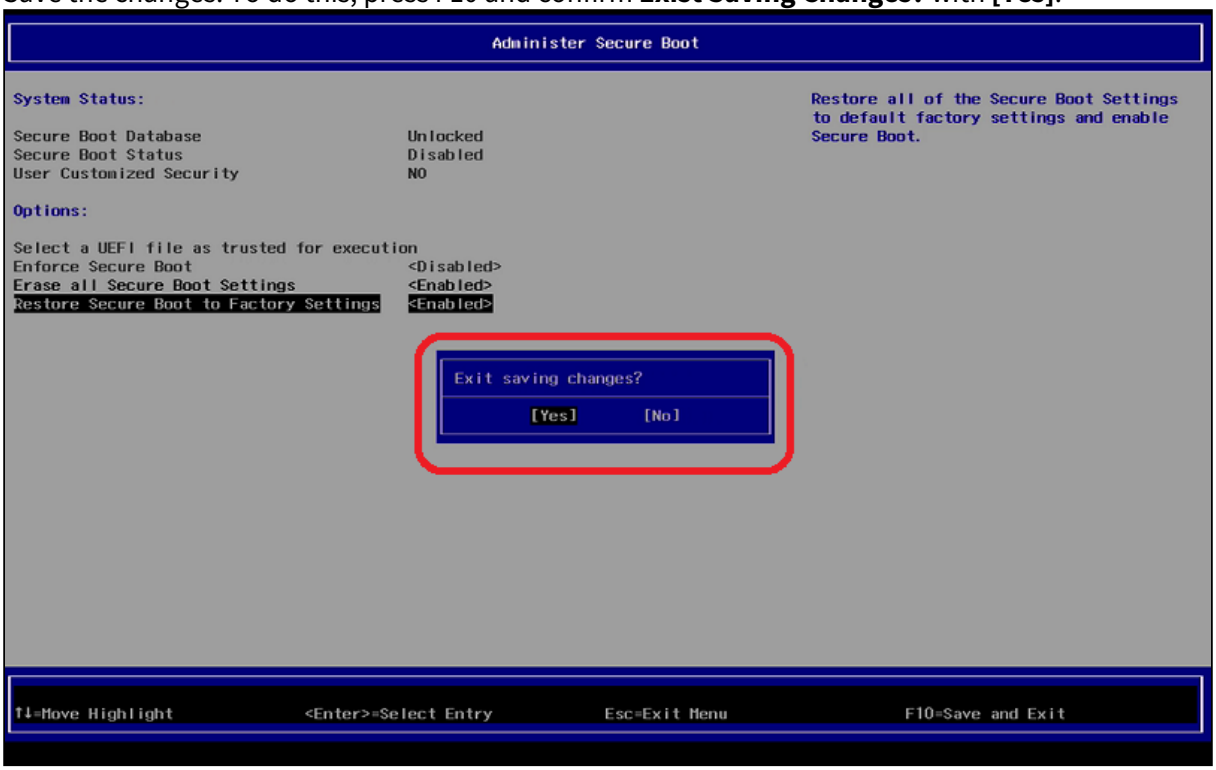
3. In the screen **Administer Secure Boot**, you will find **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** set to **<Disabled>**.



4. Change **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** to **<Enabled>**.
   If **"Enforce Secure Boot"** is not grayed out as in the picture below, change that option to as well.



5. Save the changes. To do this, press F10 and confirm **Exist Saving Changes?** with **[Yes]**.



The changes will be saved and the device will be rebooted.

6. As a last step, verify that Secure Boot is working, see Verifying that Secure Boot is Enabled (see page 280).

Enabling UEFI Secure Boot in UD3-LX 60

UEFI Secure Boot is already a default setting in UD3-LX 60.

If you have disabled secure boot, you will need to reverse the settings you made.

Enabling UEFI Secure Boot in UD6-LX 51

Prerequisites

- IGEL OS 10.04.100 or higher

> The version of IGEL OS can be found in the About window.

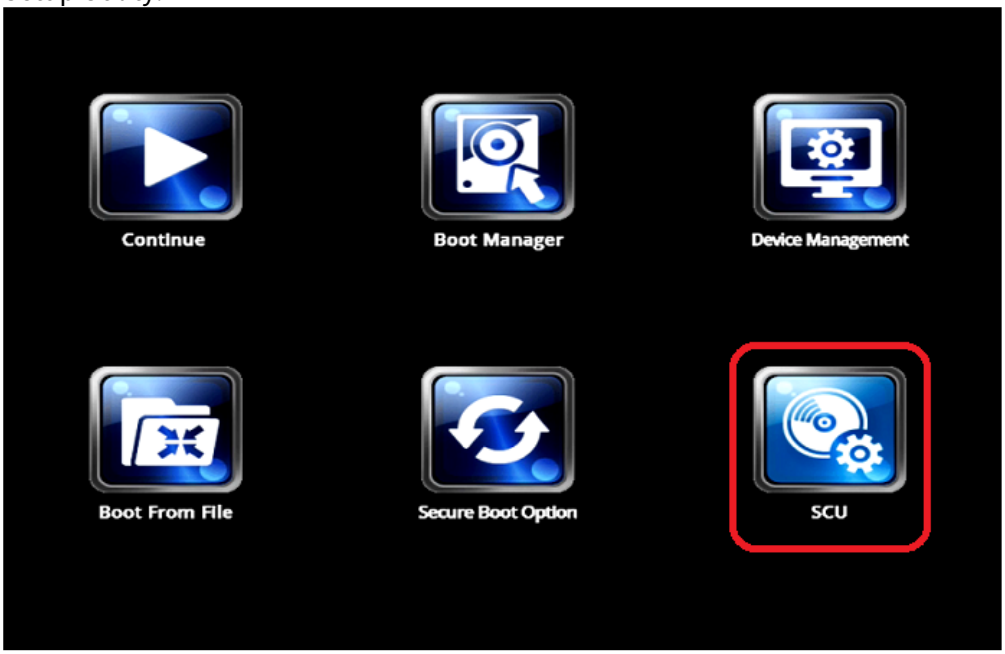
- BIOS version 3.9. 13-02202017 or higher

> To check the BIOS version, open the InsydeH20 Setup Utility as described below (step 3). Press [F9] to open the **System Information** window. In the **System Information** window, check that the BIOS version corresponds to *3.9. 13-02202017* or newer. For more information, see *Hardware > Versions of Hardware > (1-en) Hardware > (1-en) Hardware FAQs > (1-en) How Can I Update the BIOS Version?*.

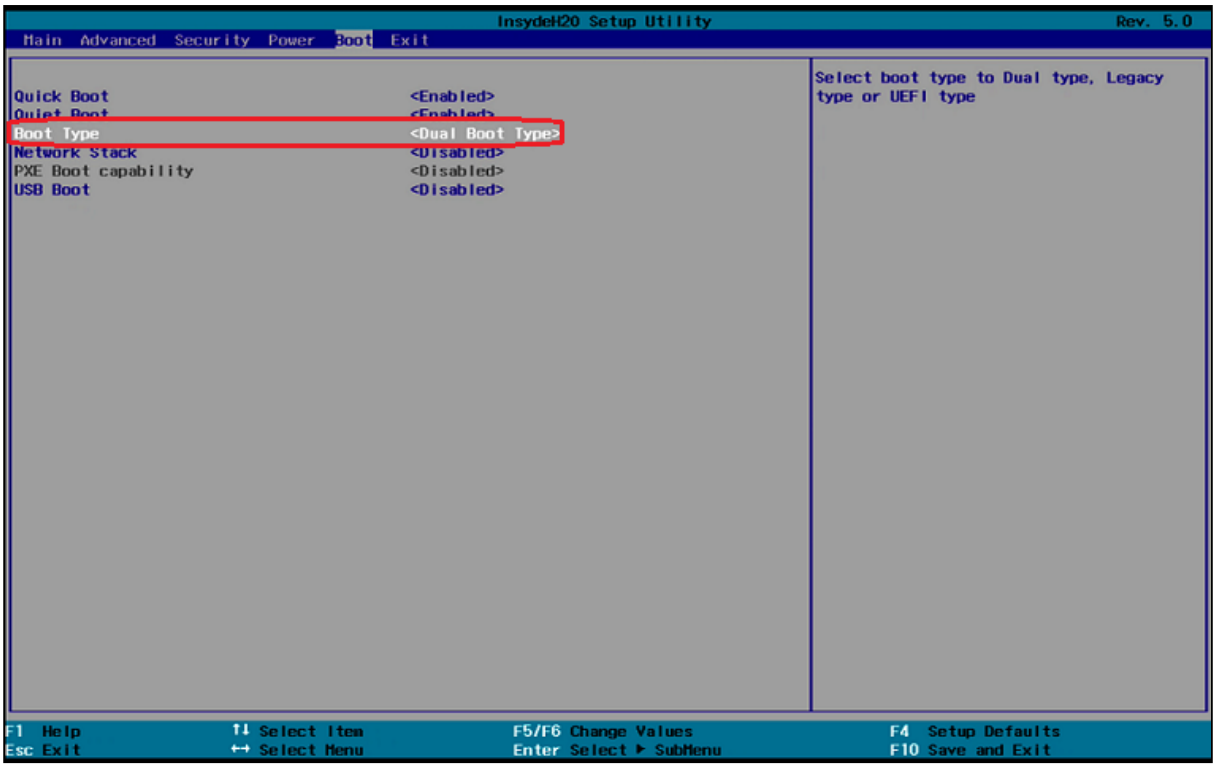
> **It is crucial to set a BIOS password to prevent users from disabling Secure Boot.**

Changing the Device's Boot Type to UEFI Boot

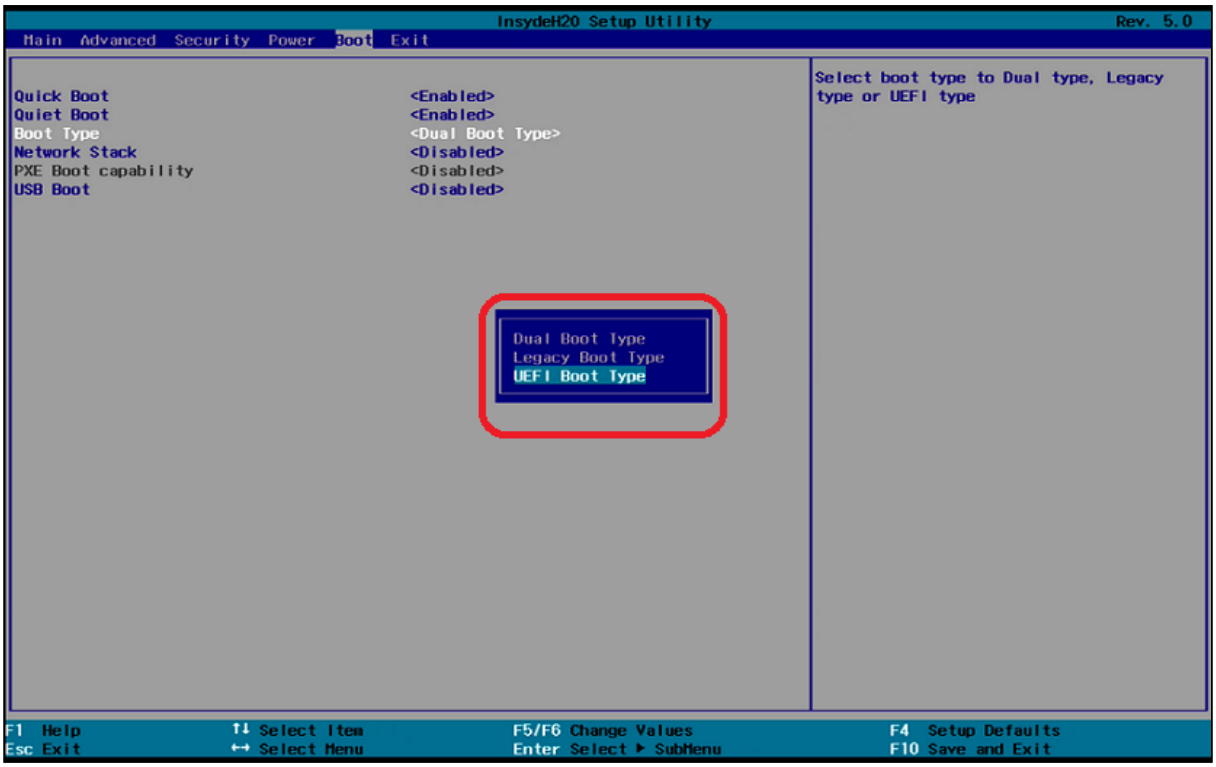
1. Turn on (or restart) the IGEL device.
2. During boot, hold the [DEL] key until you see the menu shown below.
3. Using the arrow keys, navigate to the option **SCU** and press [ENTER]. This will open the InsydeH20 Setup Utility.



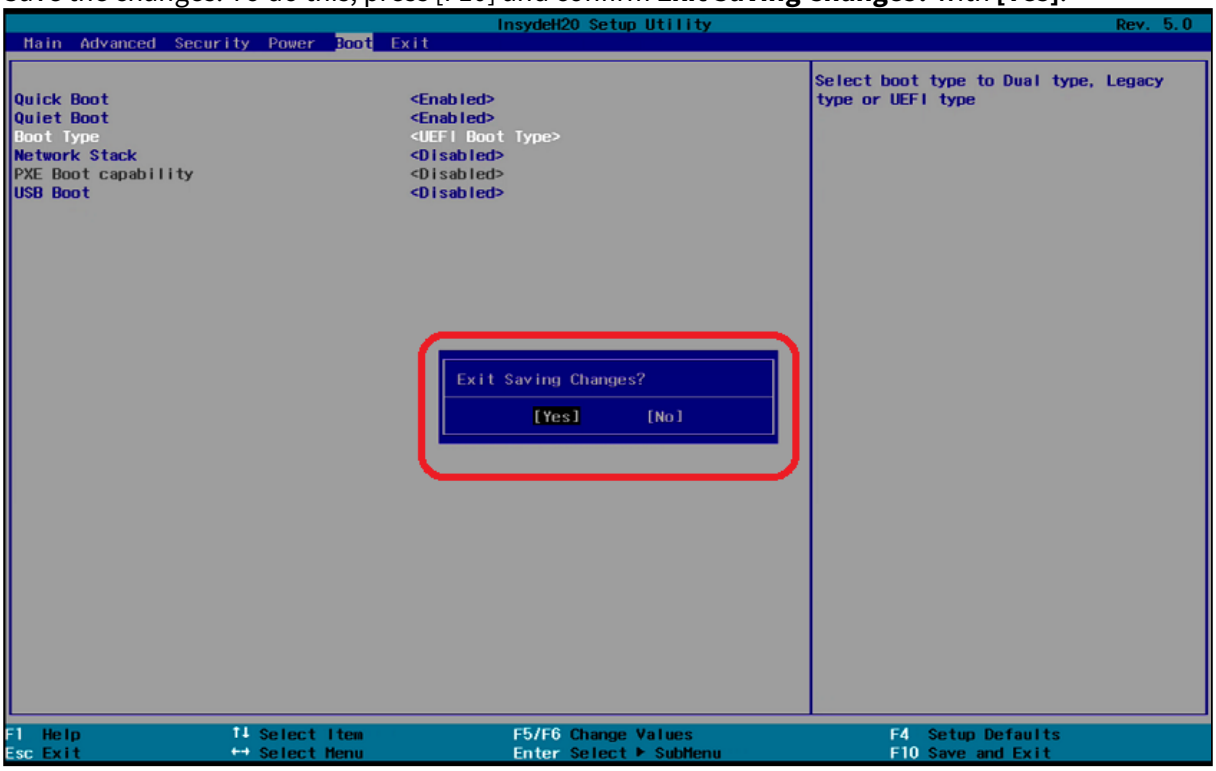
4. Using the arrow keys, move to the **Boot** tab. Ýou will find **Boot Type** set to **<Dual Boot Type>**.



5. Change **Boot Type** to **<UEFI Boot Type>**.



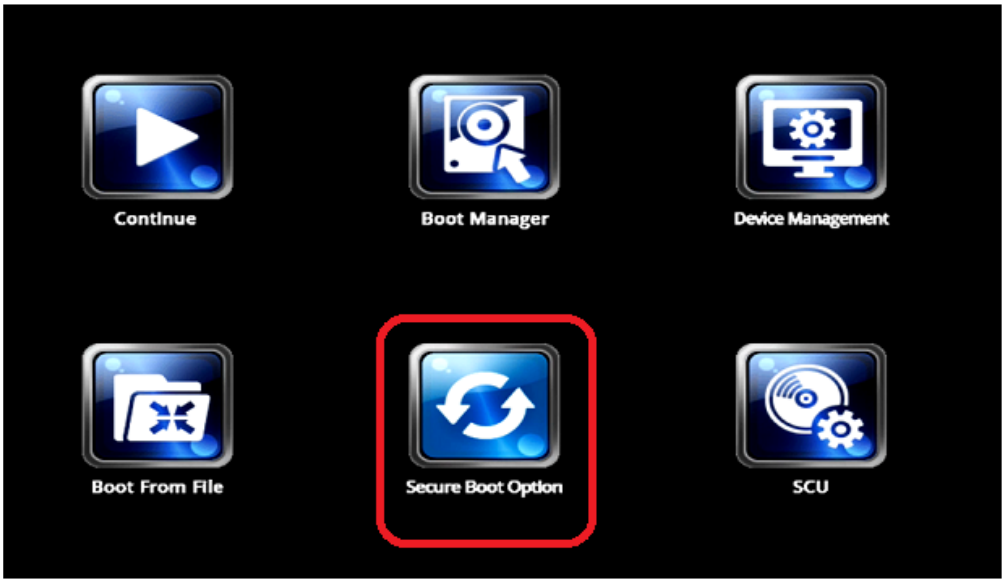
6. Save the changes. To do this, press [F10] and confirm **Exit Saving Changes?** with **[Yes]**.



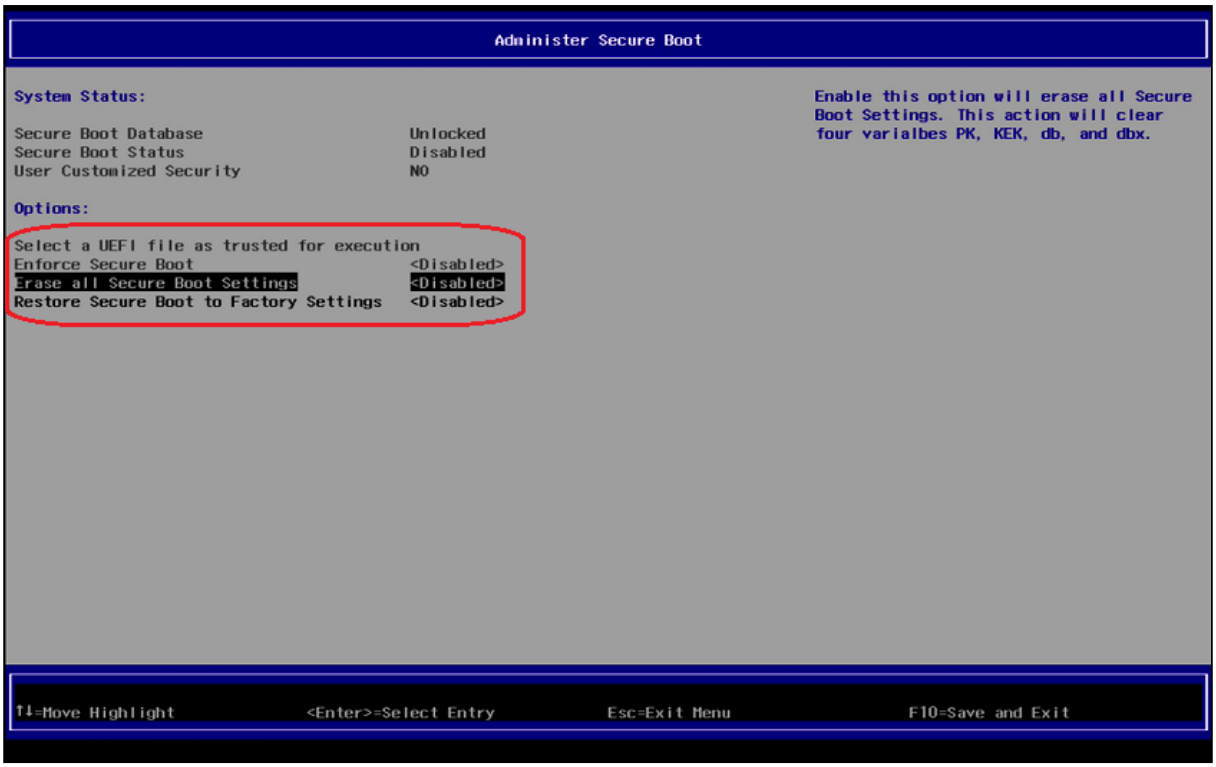
The changes will be saved and the device will be rebooted.

Activating the Secure Boot Feature

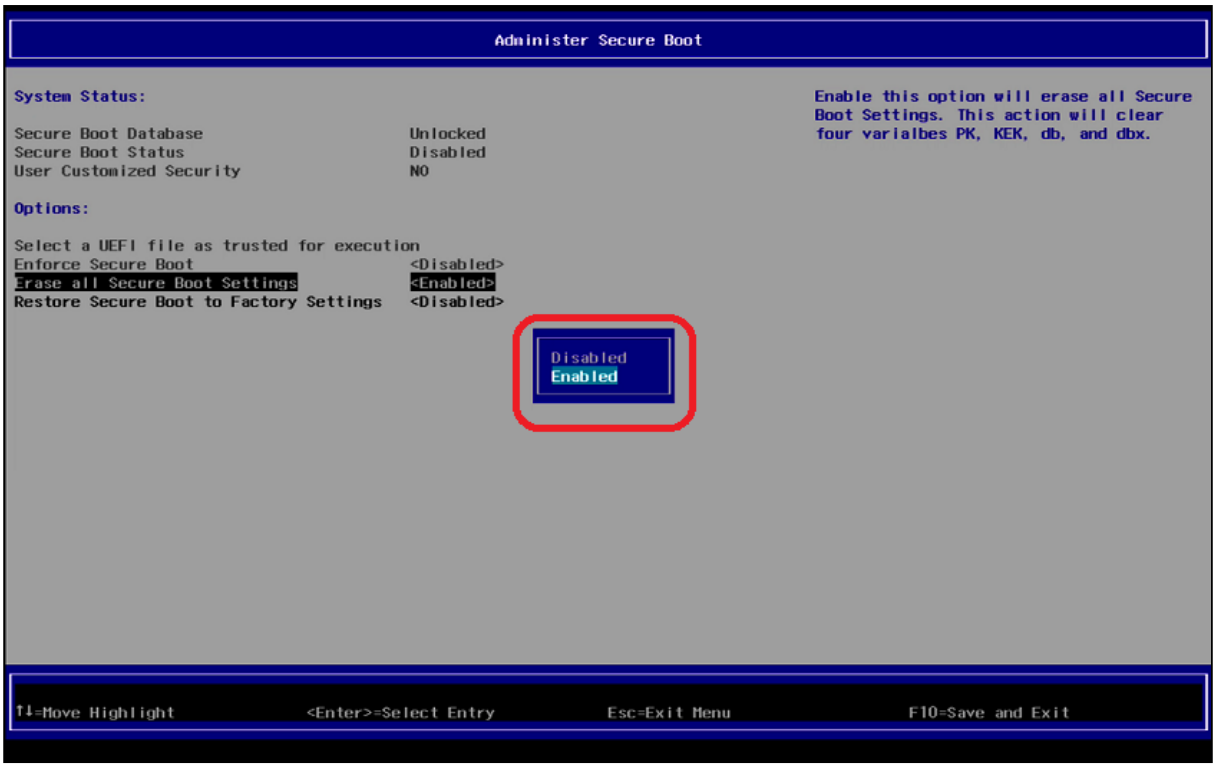
1. Turn on (or restart) the device.
2. During boot, hold the [DEL] key until you see the screen shown below.
3. Using the arrow keys, move to the option **Secure Boot Option**, and press [ENTER]. This will open the the screen **Administer Secure Boot**.



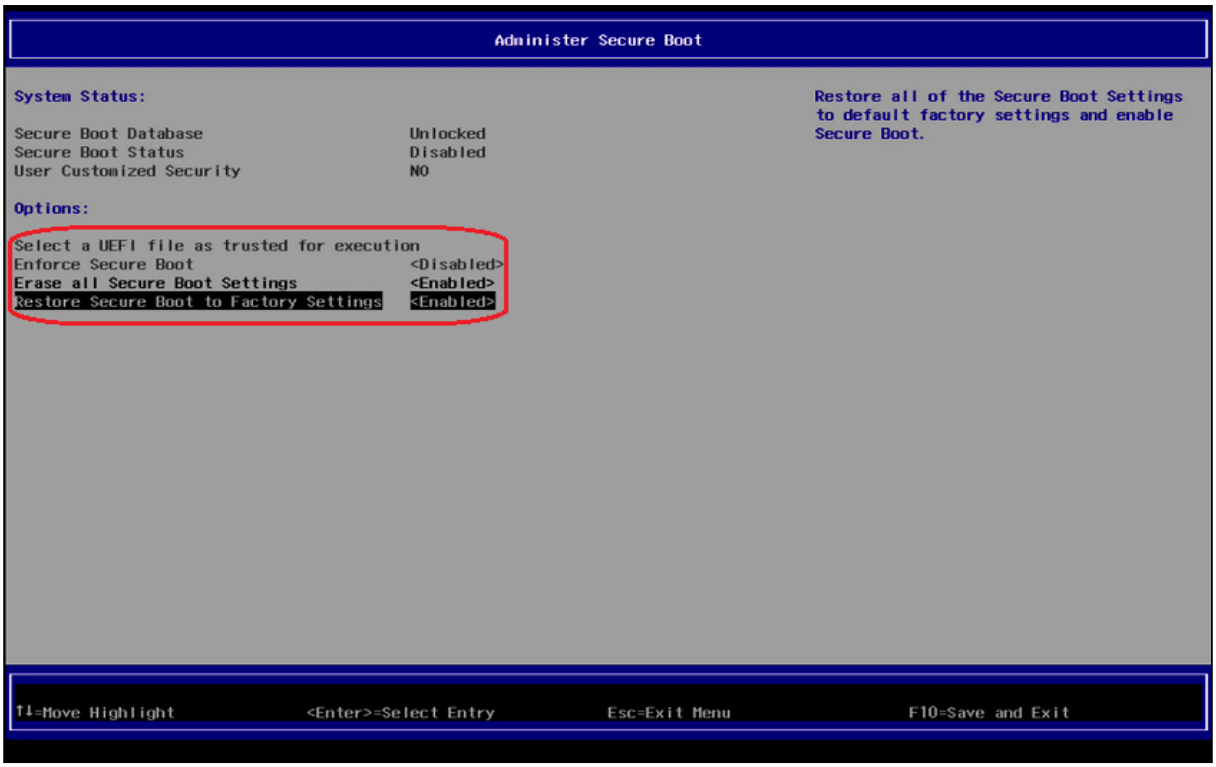
4. In the screen **Administer Secure Boot**, you will find **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** set to **<Disabled>**.



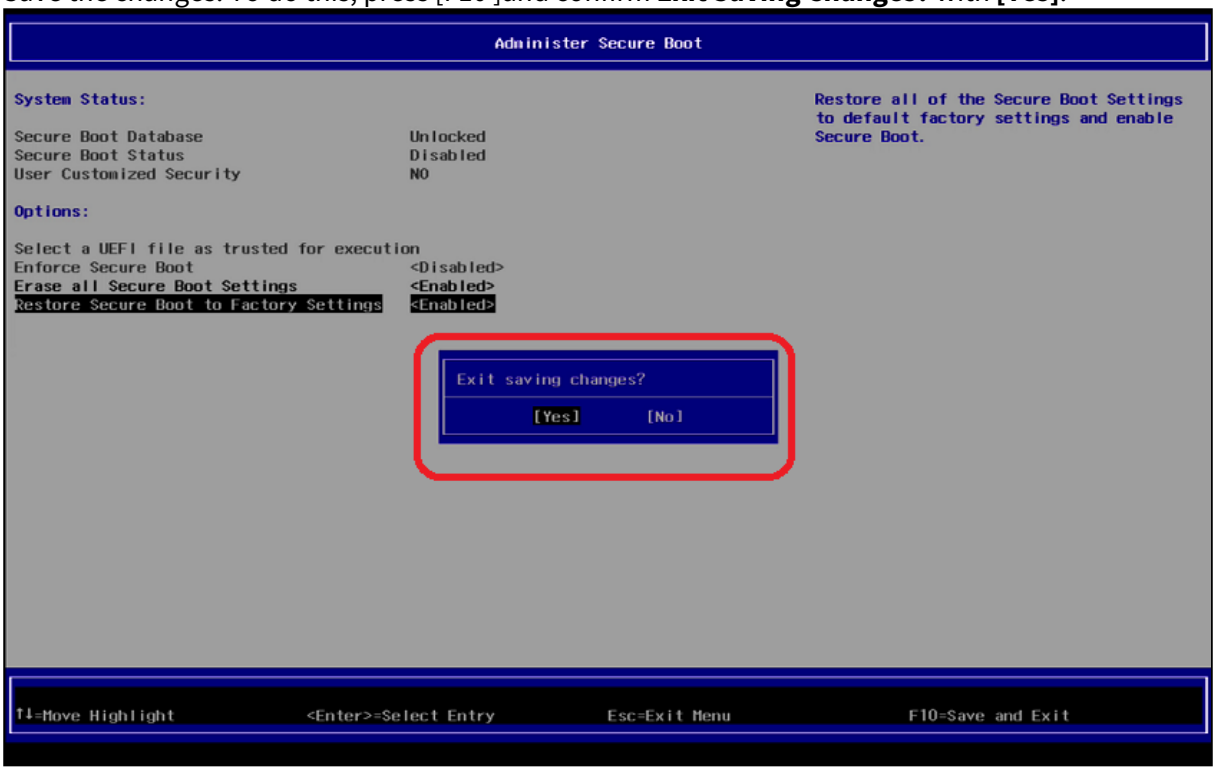
5. In the screen **Administer Secure Boot**, set "**Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** to **<Enabled>**.



6. **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** are now set to **<Enabled>**.
   If **"Enforce Secure Boot"** is not grayed out as in the picture below, change that option to as well.



7. Save the changes. To do this, press [F10]and confirm **Exit Saving Changes?** with **[Yes]**.



The changes will be saved and the device will be rebooted.

8. As a last step, verify that Secure Boot is working, see Verifying that Secure Boot is Enabled (see page 280).

Enabling UEFI Secure Boot in UD7-LX 10

Prerequisites

- IGEL OS 10.04.100 or higher

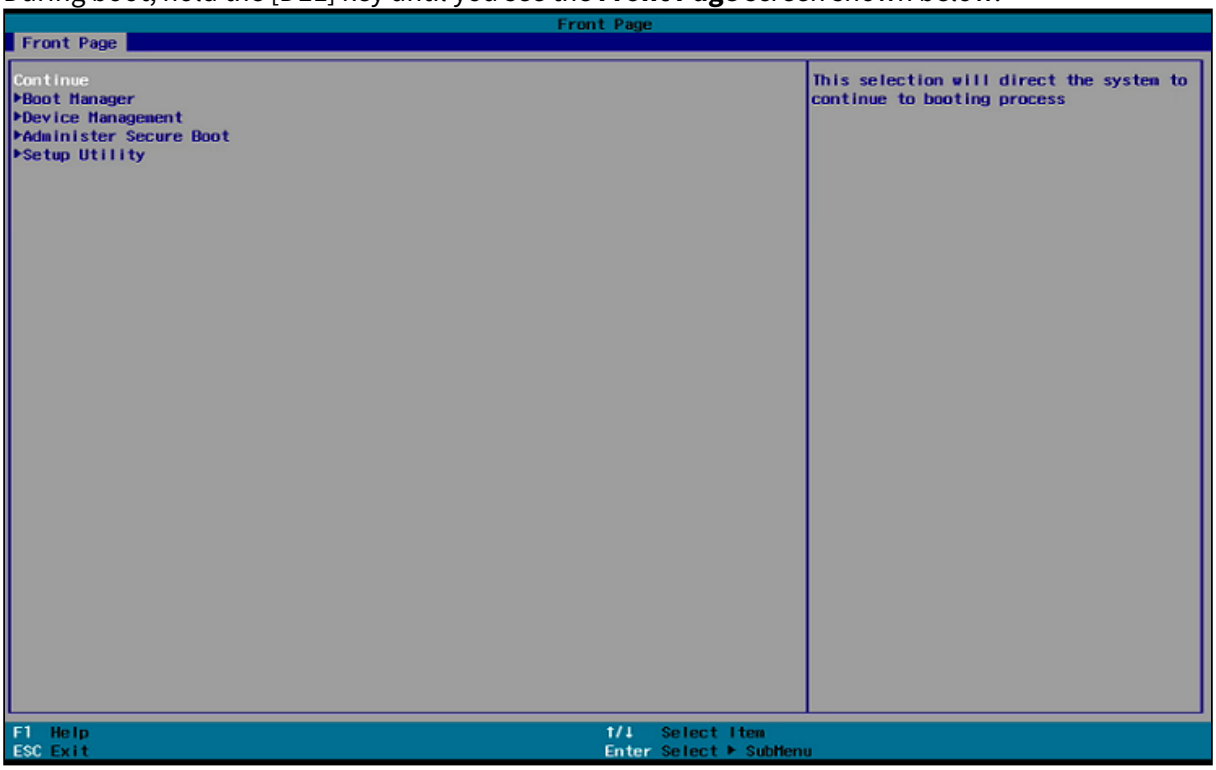
> The version of IGEL Linux can be found in the **About** window.

> UD7-LX 10 supports UEFI Secure Boot by default and no BIOS update is necessary.

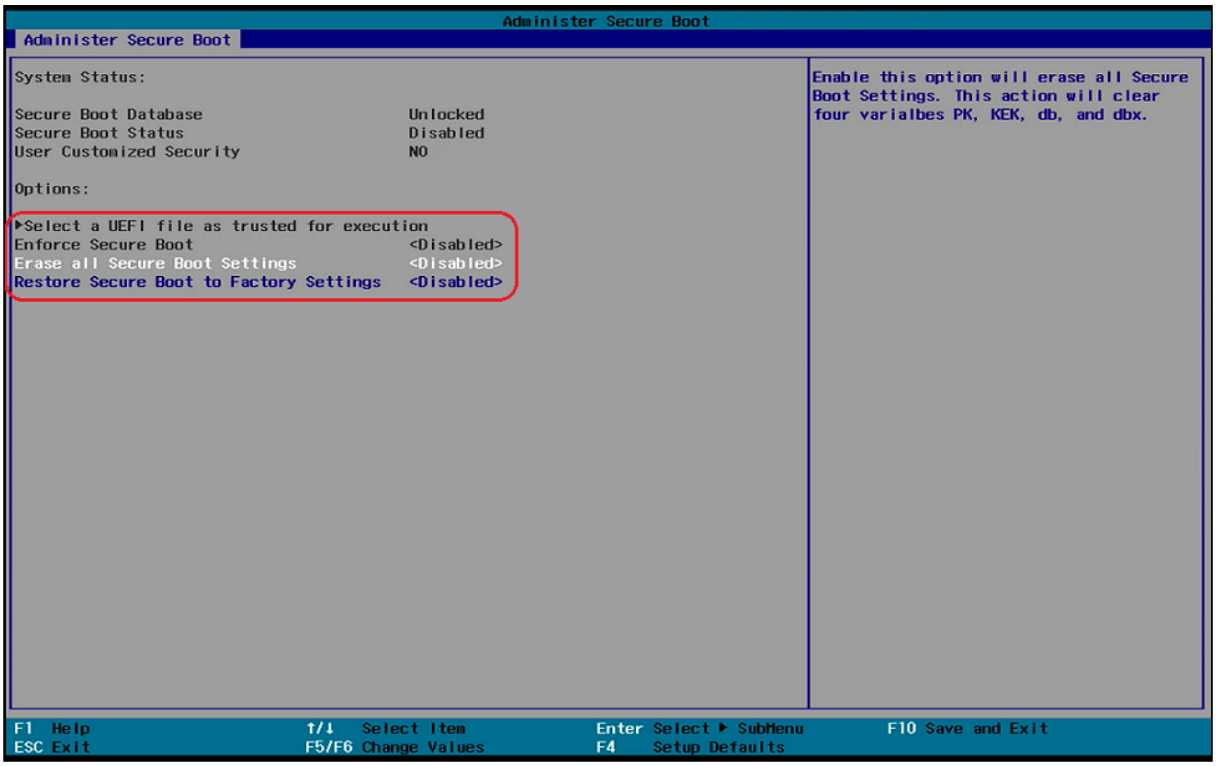
> **It is crucial to set a BIOS password to prevent users from disabling Secure Boot.**

Activating the Secure Boot Feature

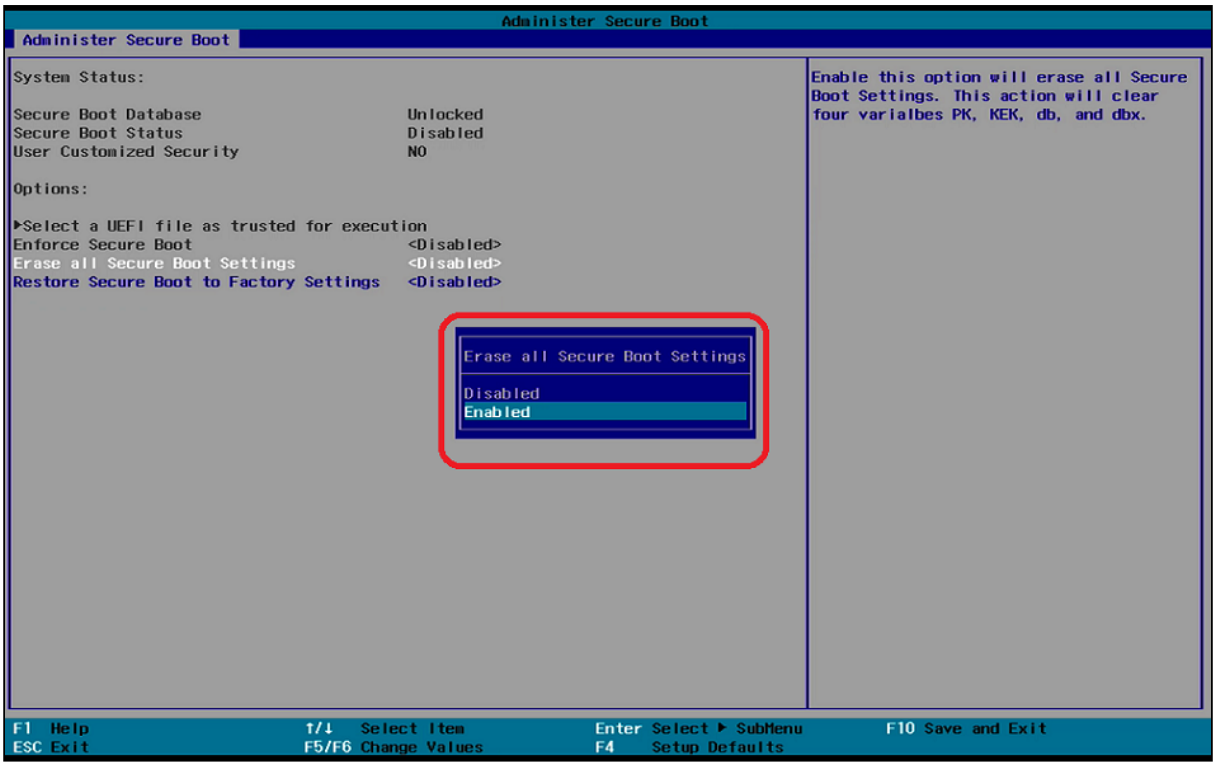
1. Turn on (or restart) the IGEL device.
2. During boot, hold the [DEL] key until you see the **Front Page** screen shown below.



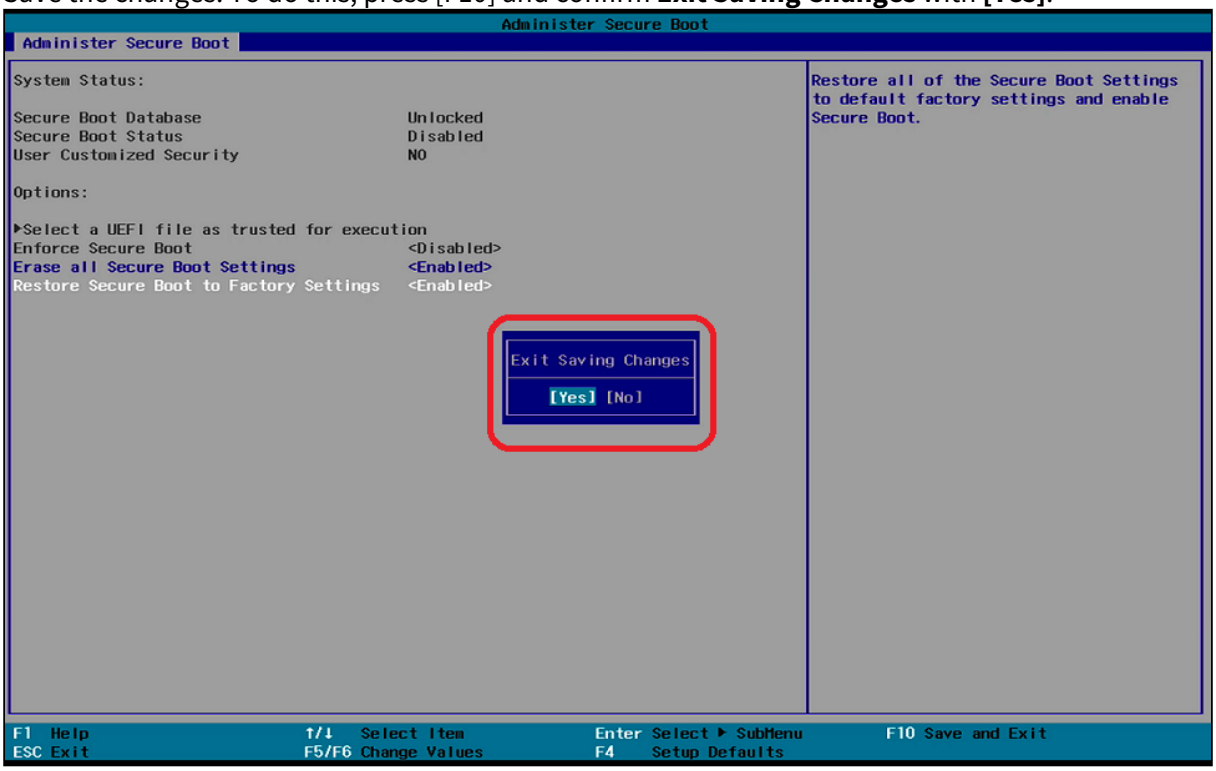
3. In the **Administer Secure Boot** screen, you will find **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** set to **<Disabled>**.



4. Change both **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** to **<Enabled>**.
   If **"Enforce Secure Boot"** is not grayed out as in the picture below, change that option to as well.



5. Save the changes. To do this, press [F10] and confirm **Exit Saving Changes** with **[Yes]**.



The changes will be saved and the device will be rebooted.

6. As a last step, verify that Secure Boot is working, see Verifying that Secure Boot is Enabled (see page 280) .

Enabling UEFI Secure Boot in UD7-LX 20

UEFI Secure Boot is already a default setting in UD7-LX 20.

If you have disabled secure boot, you will need to reverse the settings you made.

Microsoft Windows 10 IoT

Enabling UEFI Secure Boot in UD3-W10 51

Prerequisites

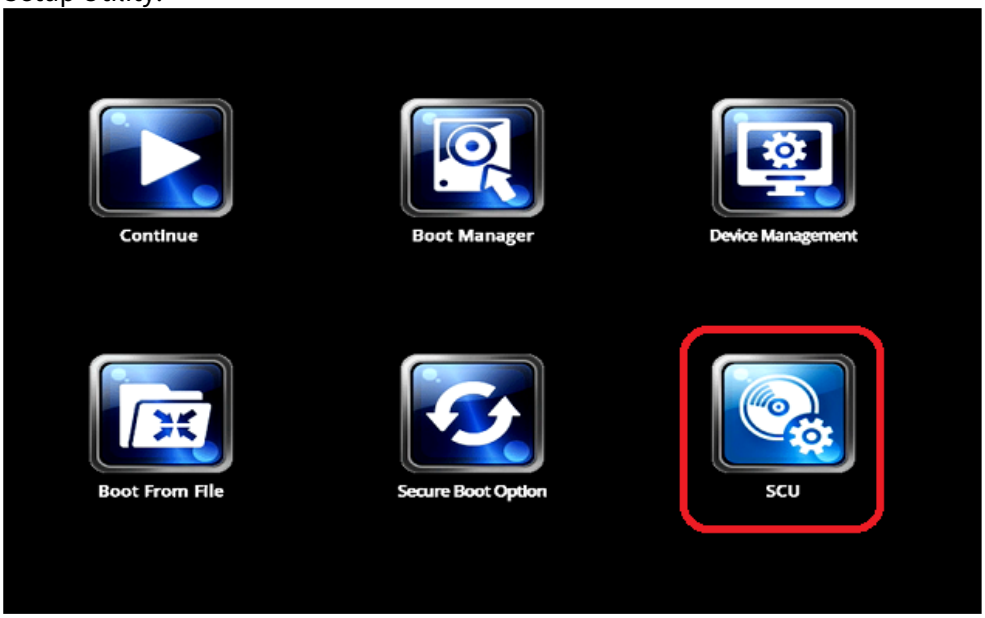
- Microsoft Windows IoT 4.03.100 or higher
- BIOS version 3.A. 13-11202017 or higher

To check the BIOS version, open the InsydeH20 Setup Utility as described below (step 3). Press [F9] to open the **System Information** window. In the **System Information** window, check that the BIOS version corresponds to *3.A. 13-11202017* or newer. For more information, see *Hardware > Versions of Hardware > (1-en) Hardware > (1-en) Hardware FAQs > (1-en) How Can I Update the BIOS Version?*.

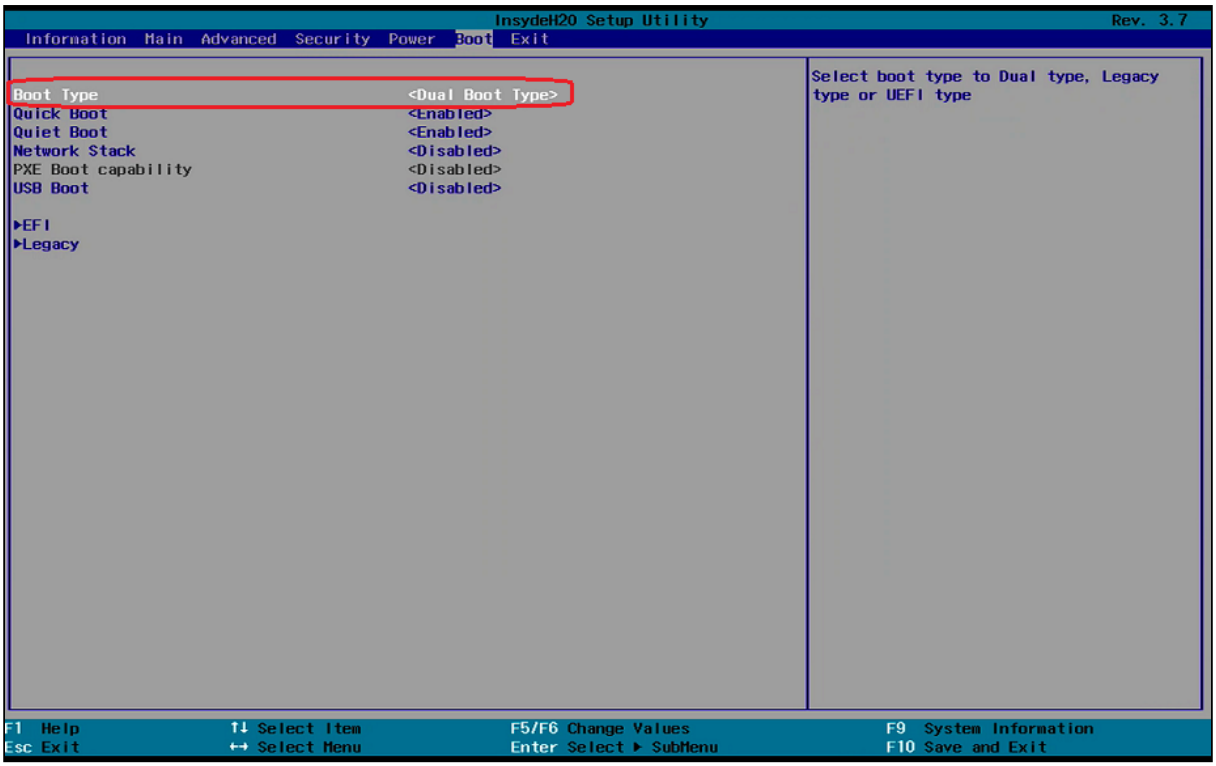
It is crucial to set a BIOS password to prevent users from disabling Secure Boot.

Changing the Device's Boot Type to UEFI Boot

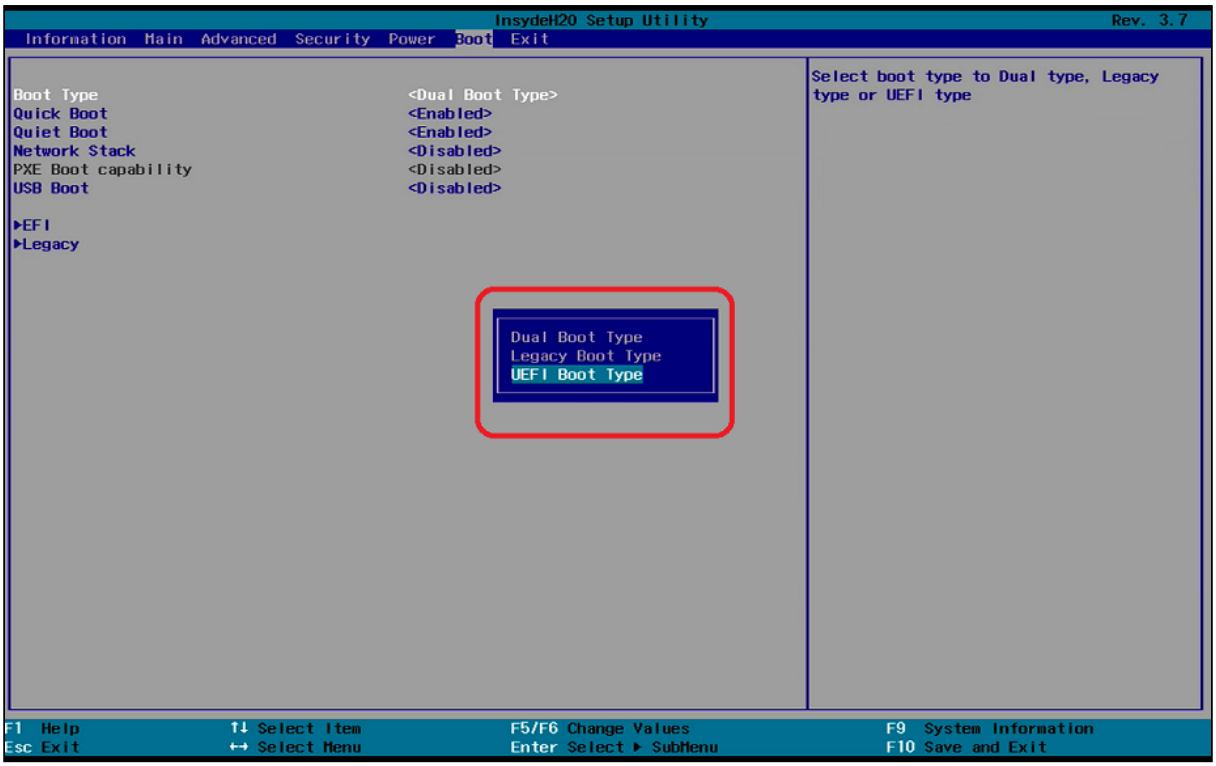
1. Turn on (or restart) the IGEL device.
2. During boot, hold the [DEL] key until you see the menu shown below.
3. Using the arrow keys, navigate to the option **SCU** and press [ENTER]. This will open the InsydeH20 Setup Utility.



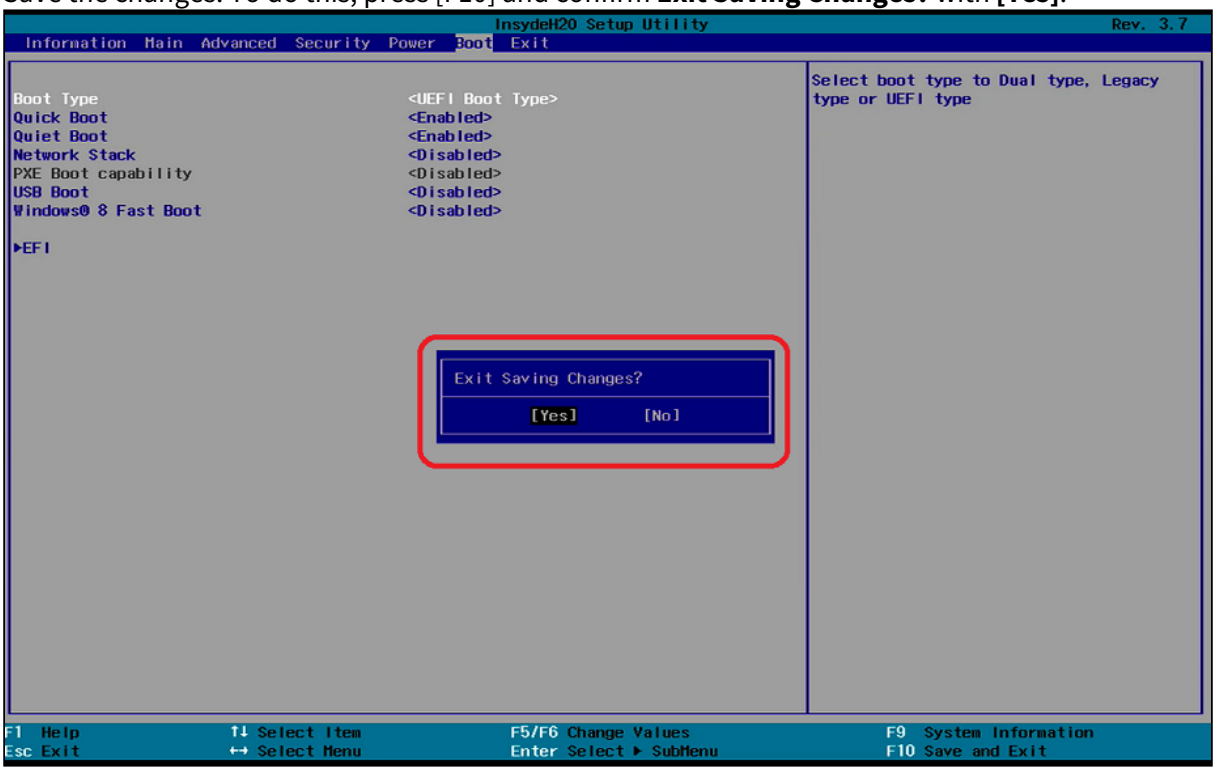
4. Using the arrow keys, move to the tab **Boot**. You will find **Boot Type** set to **<Dual Boot Type>**.



5. Change **Boot Type** to **<UEFI Boot Type>**.



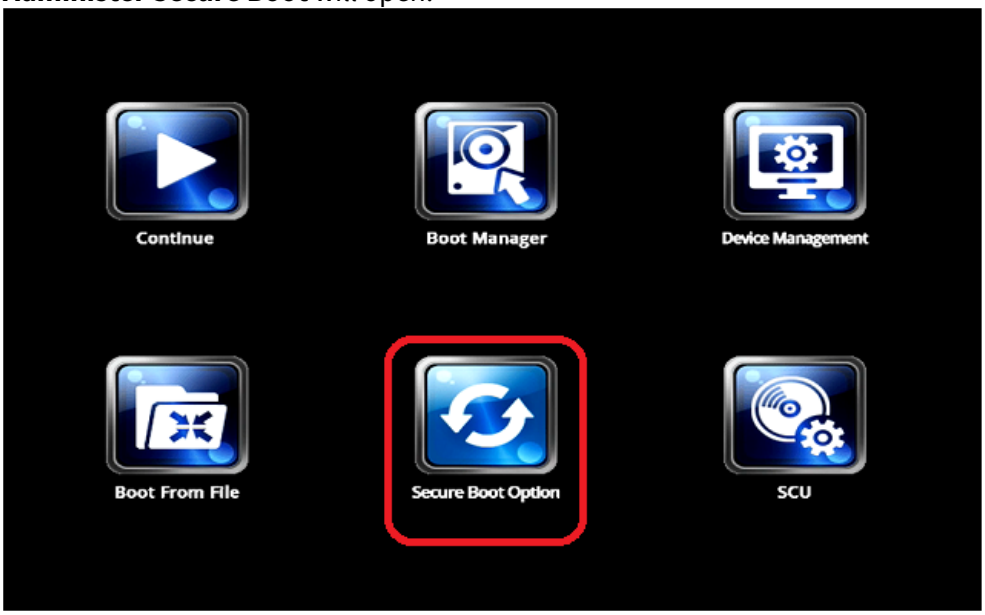
6. Save the changes. To do this, press [F10] and confirm **Exit Saving Changes?** with **[Yes]**.



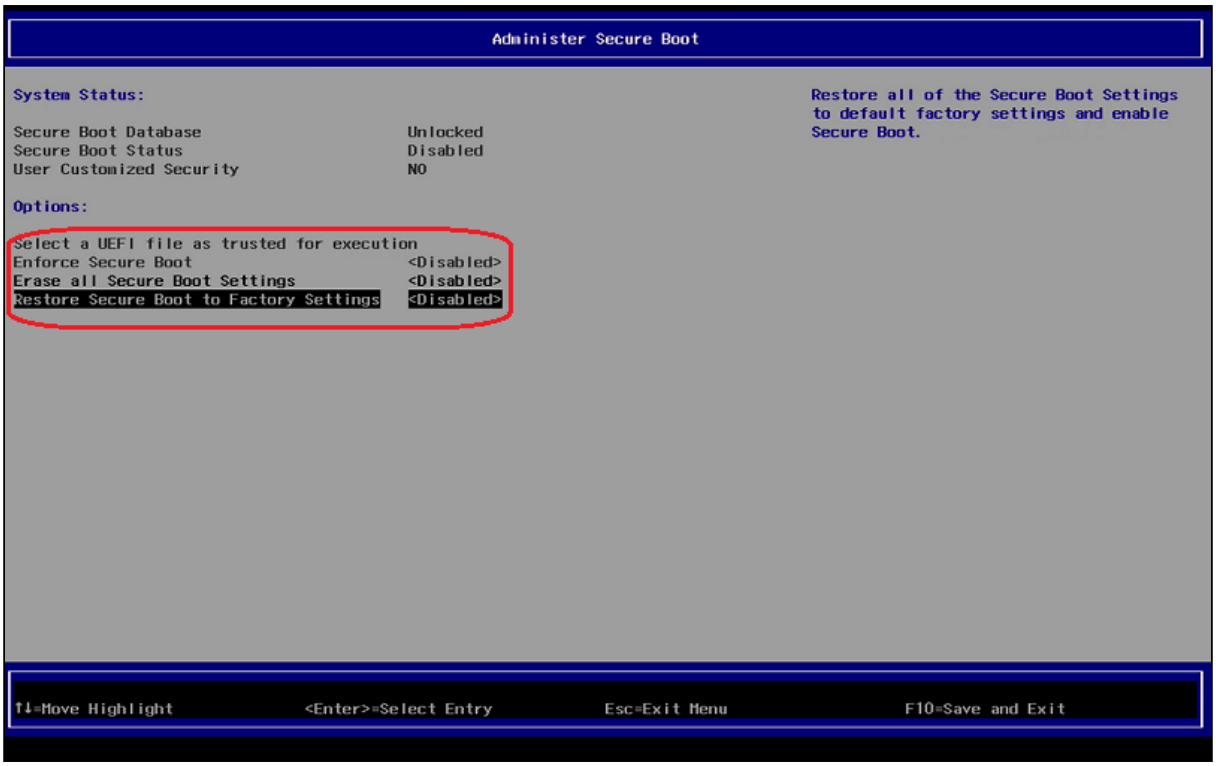
The changes will be saved and the device will be rebooted.

Activating the Secure Boot Feature

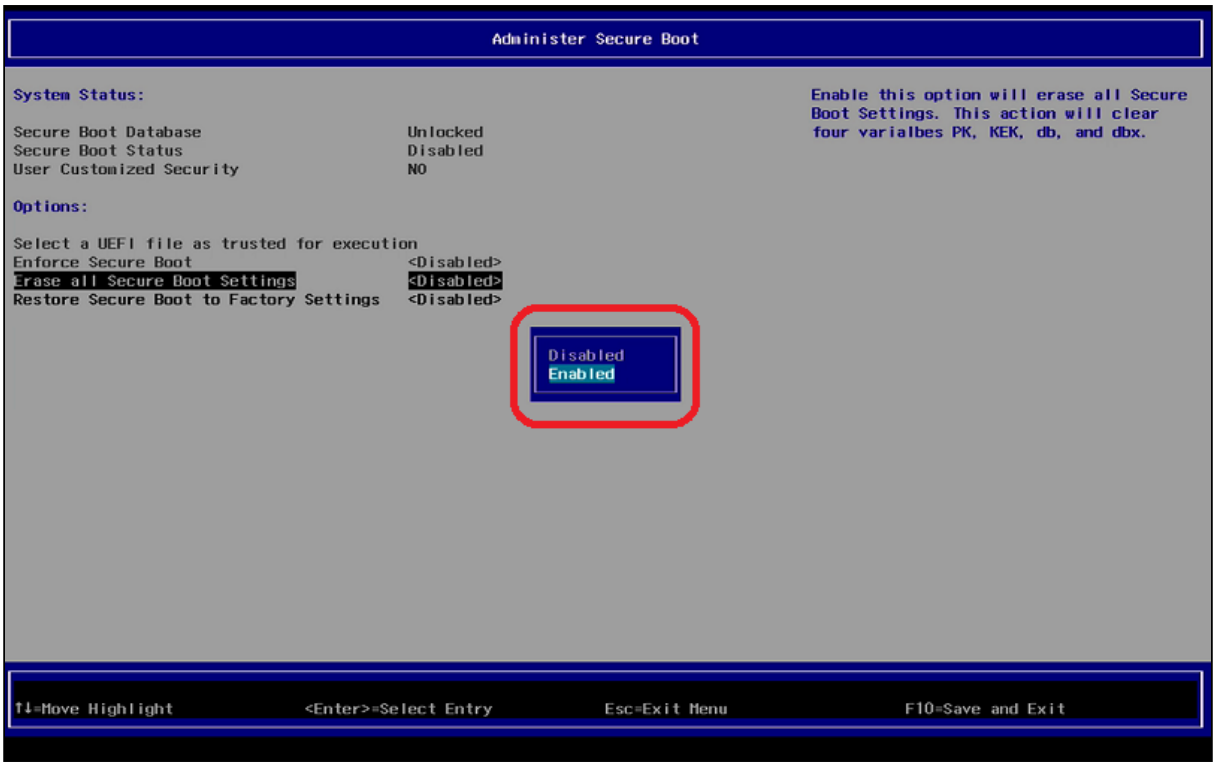
1. Turn on (or restart) the IGEL device.
2. Using the arrow keys, move to **Secure Boot Option** and press [ENTER]. The BIOS screen **Administer Secure Boot** will open.



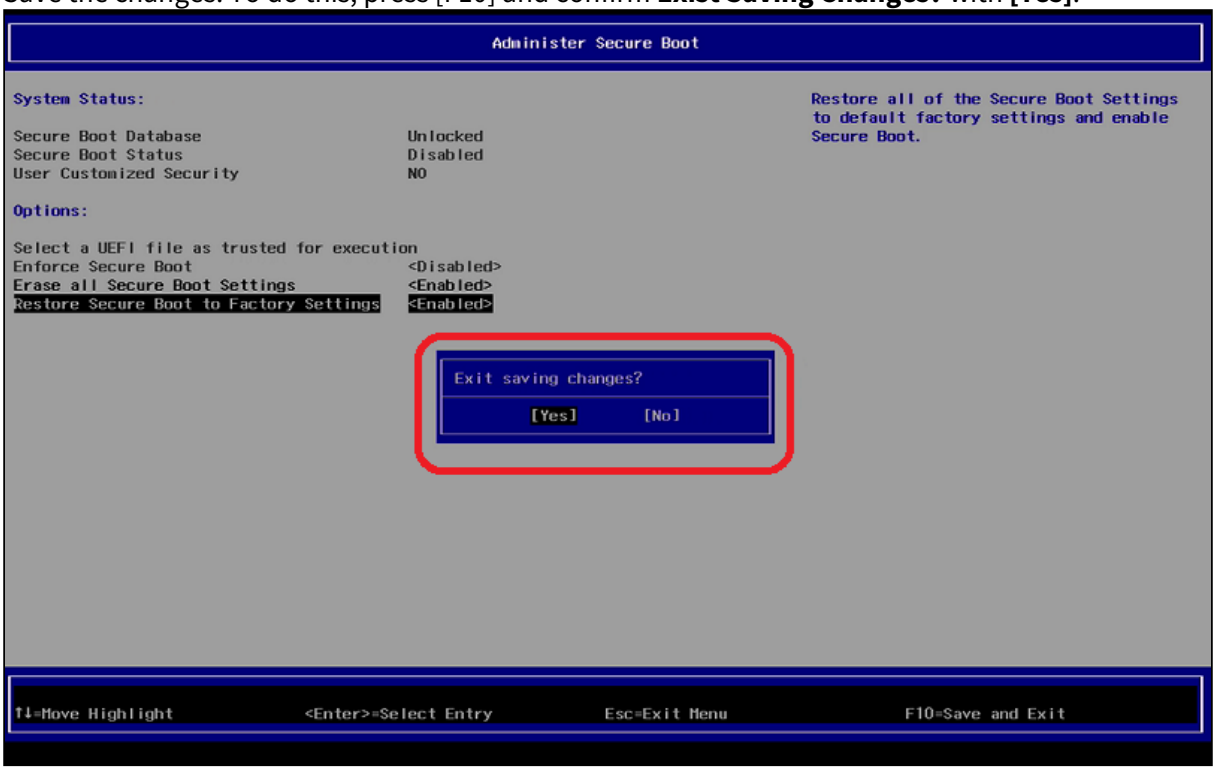
3. In the screen **Administer Secure Boot**, you will find **Erase all Secure Boot Settings** and **Restore Secure Boot to Factory Settings** set to **<Disabled>**.



4. Change **Erase all Secure Boot Settings** and **Restore Secure Boot to Factory Settings** to **<Enabled>**.
   If **Enforce Secure Boot** is not grayed out as in the picture below, change that option to as well.



5. Save the changes. To do this, press [F10] and confirm **Exist Saving Changes?** with **[Yes]**.



The changes will be saved and the device will be rebooted.

6. As a last step, verify that Secure Boot is working, see Verifying that Secure Boot is Enabled (see page 280).

Enabling UEFI Secure Boot in UD6-W10 51

Prerequisites

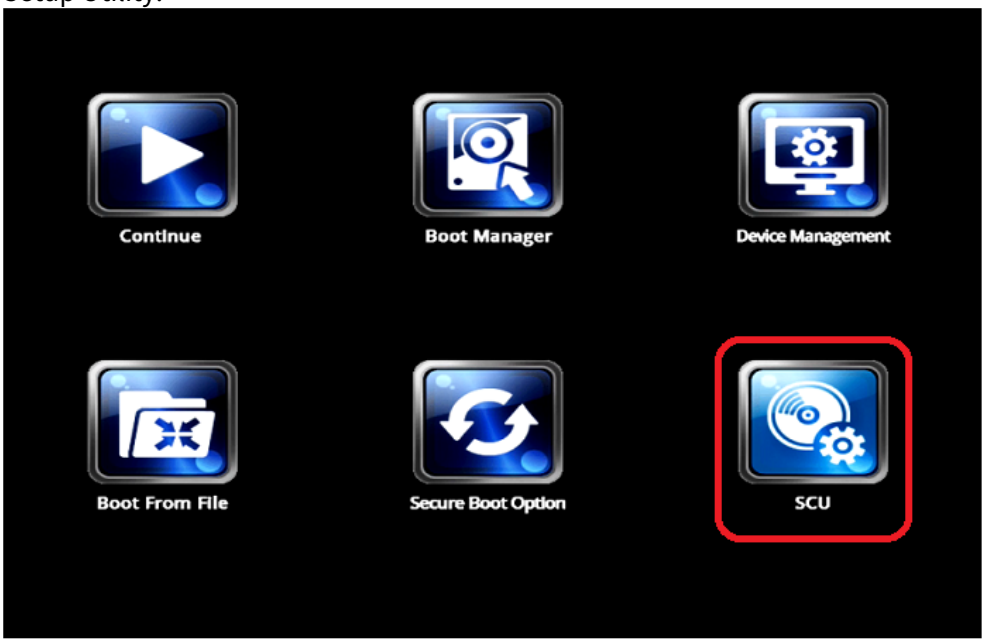
- Microsoft Windows 10 IoT 4.03.100 or higher
- BIOS version 3.9. 13-02202017 or higher

To check the BIOS version, open the InsydeH20 Setup Utility as described below (step 3). Press [F9] to open the **System Information** window. In the **System Information** window, check that the BIOS version corresponds to *3.9. 13-02202017* or newer. For more information, see *Hardware* > *Versions of Hardware* > *(1-en) Hardware* > *(1-en) Hardware FAQs* > *(1-en) How Can I Update the BIOS Version?*.

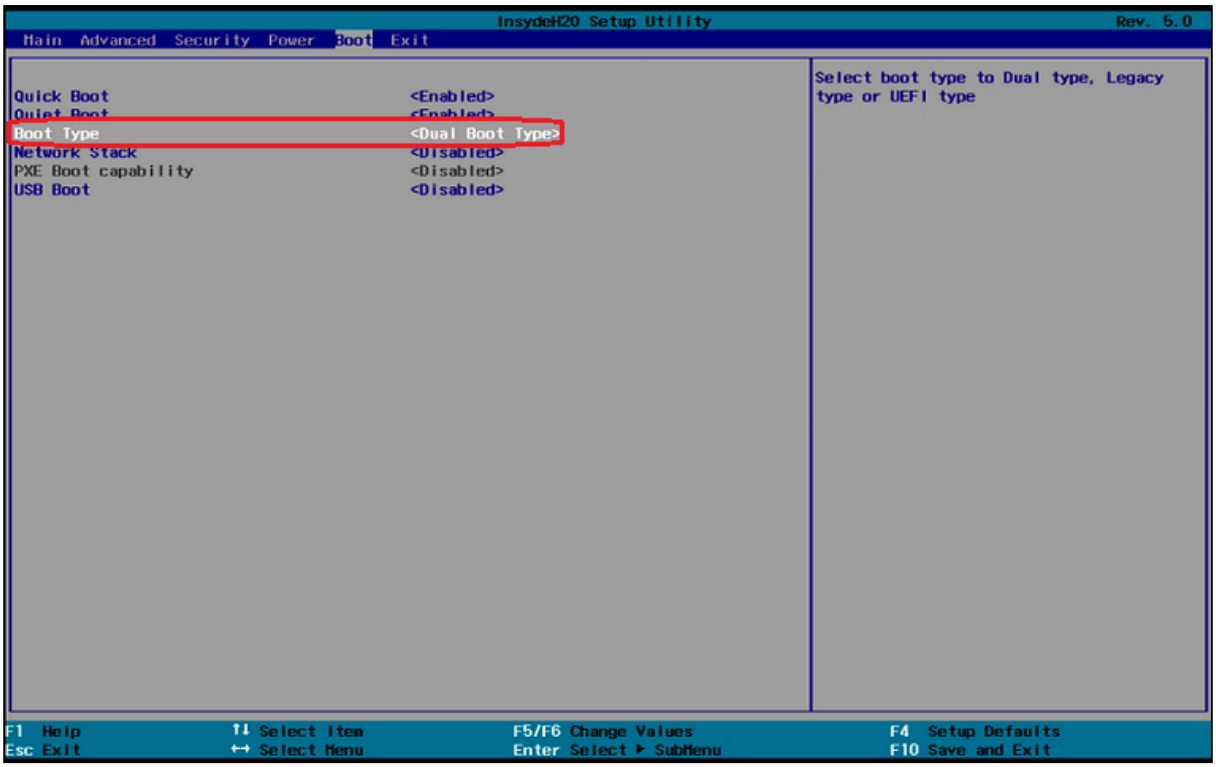
It is crucial to set a BIOS password to prevent users from disabling Secure Boot.

Changing the Device's Boot Type to UEFI Boot

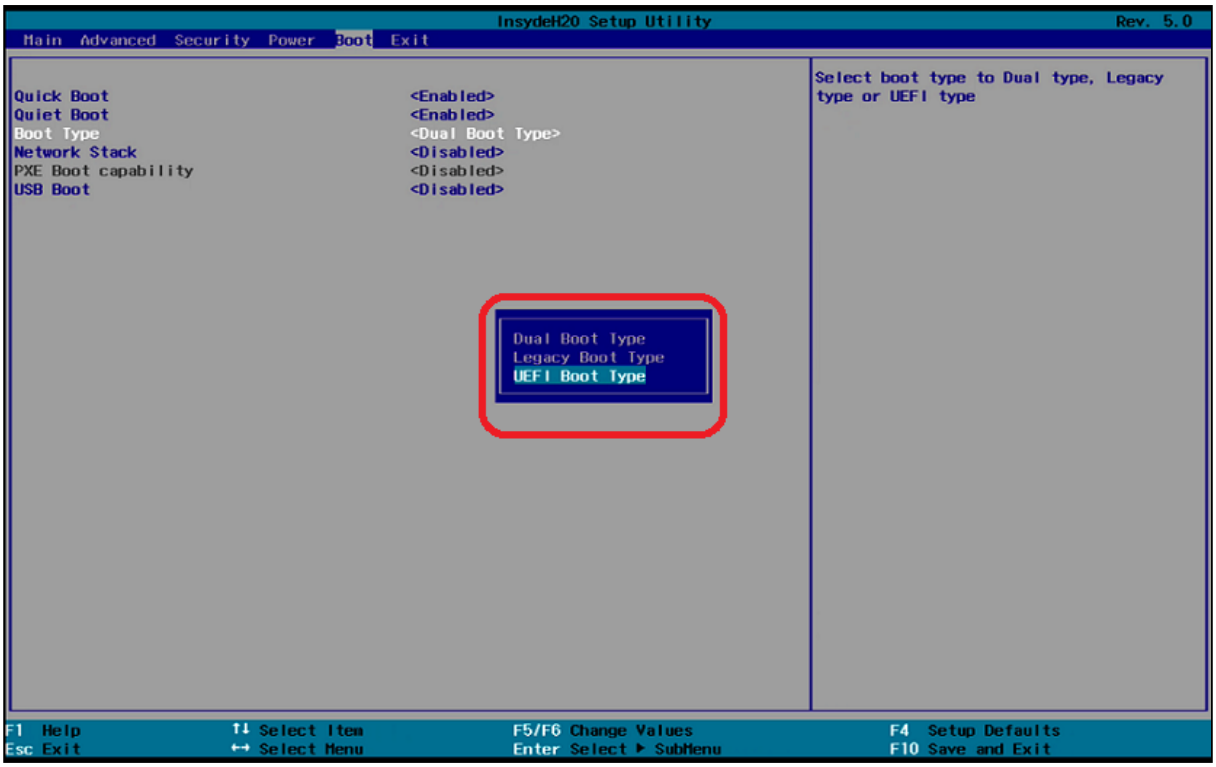
1. Turn on (or restart) the IGEL device.
2. During boot, hold the [DEL] key until you see the menu shown below.
3. Using the arrow keys, navigate to the option **SCU** and press [ENTER]. This will open the InsydeH20 Setup Utility.



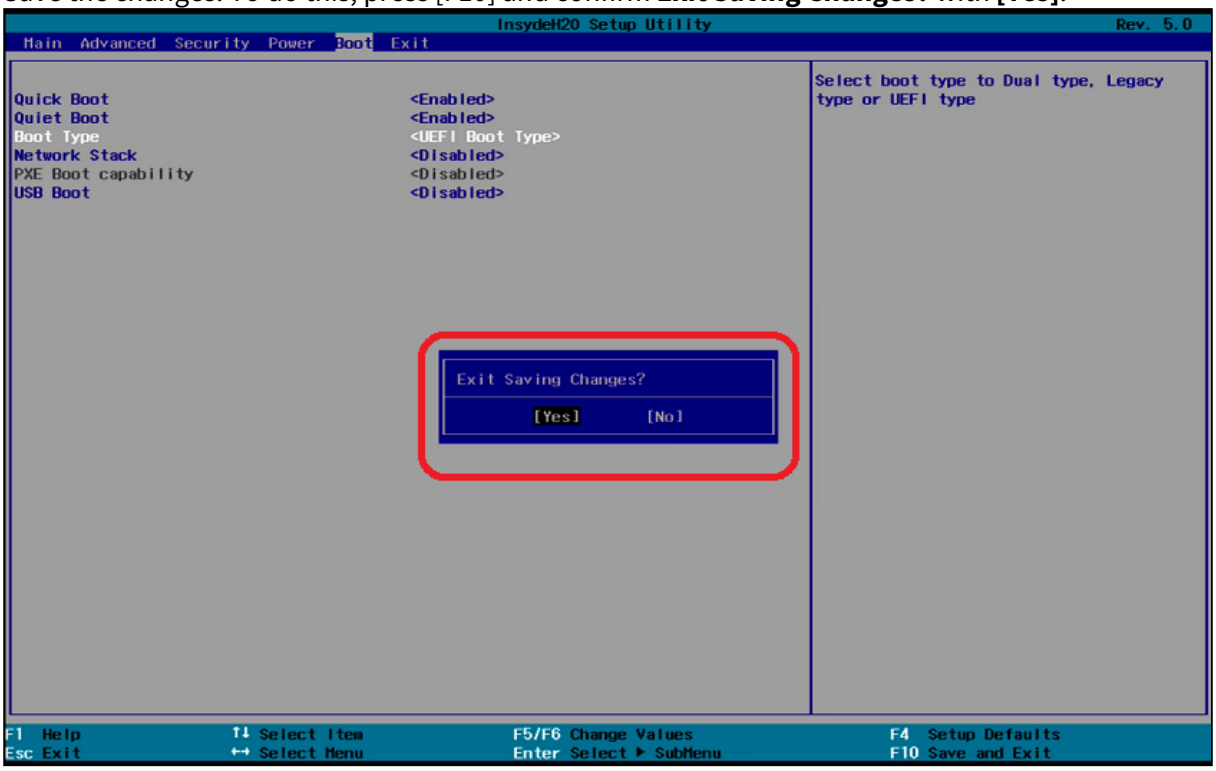
4. Using the arrow keys, move to the **Boot** tab. You will find **Boot Type** set to **<Dual Boot Type>**.



5. Change **Boot Type** to **<UEFI Boot Type>**.



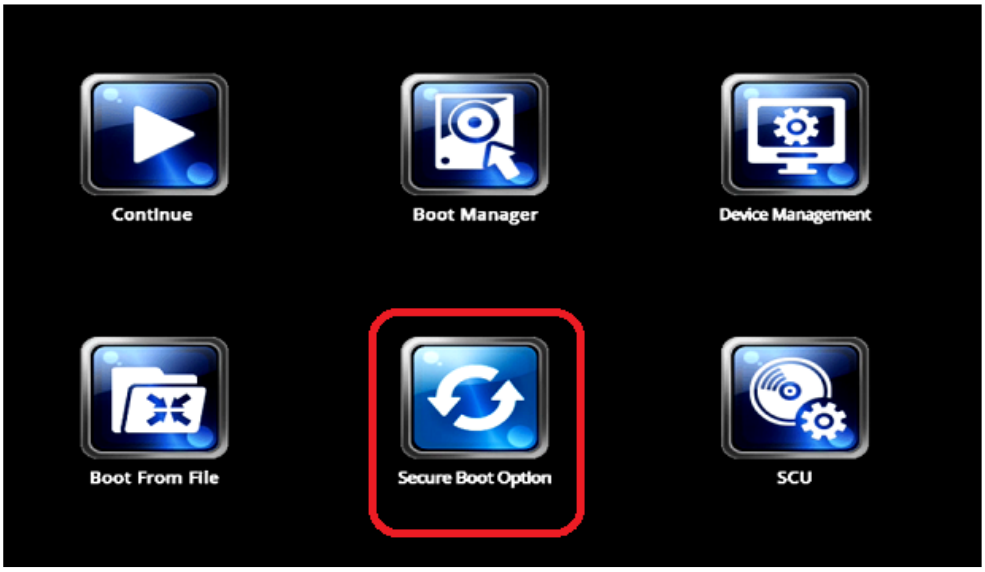
6. Save the changes. To do this, press [F10] and confirm **Exit Saving Changes?** with **[Yes]**.



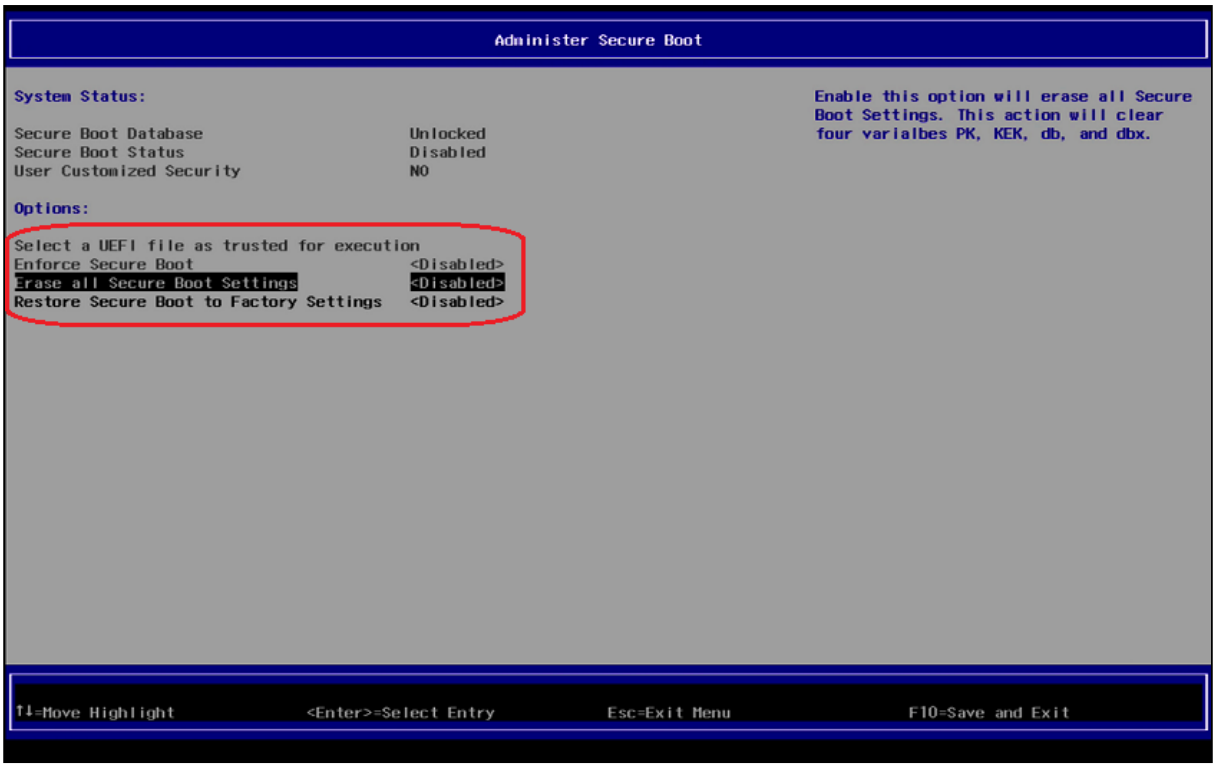
The changes will be saved and the device will be rebooted.

Activating the Secure Boot Feature

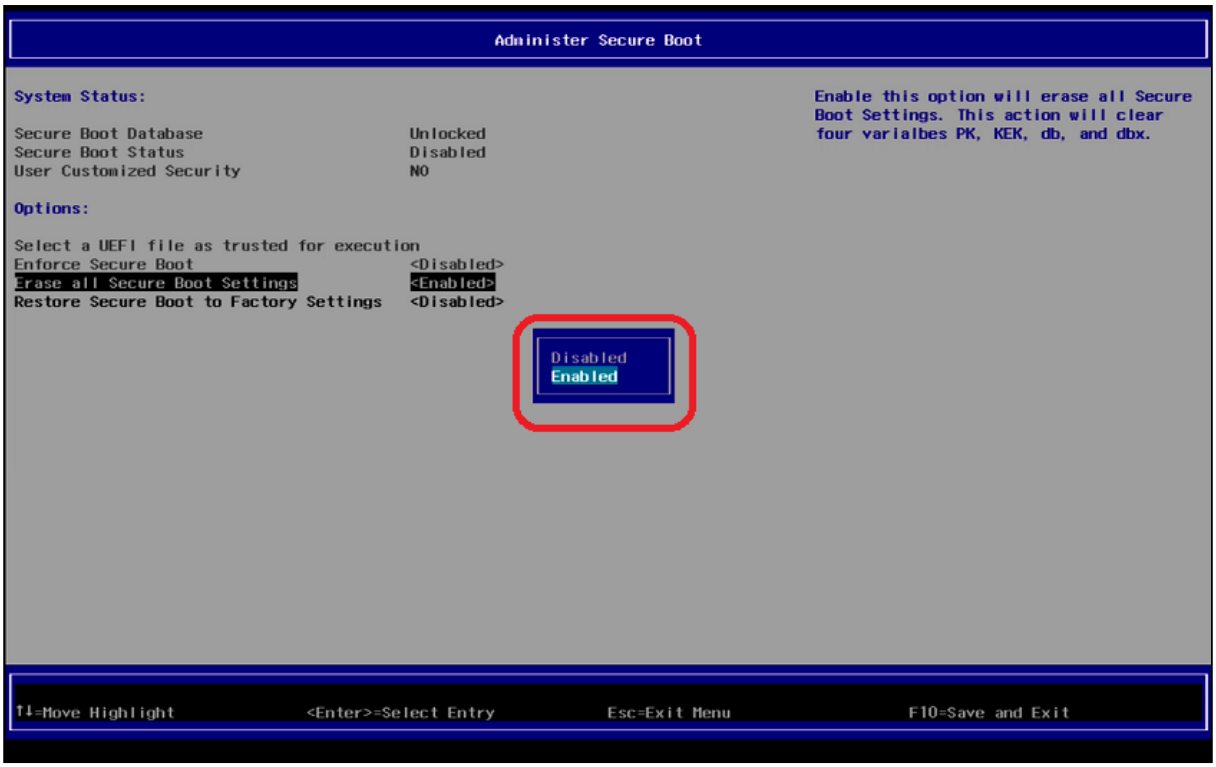
1. Turn on (or restart) the device.
2. During boot, hold the [DEL] key until you see the screen shown below.
3. Using the arrow keys, move to the option **Secure Boot Option** and press [ENTER]. This will open the the screen **Administer Secure Boot**.



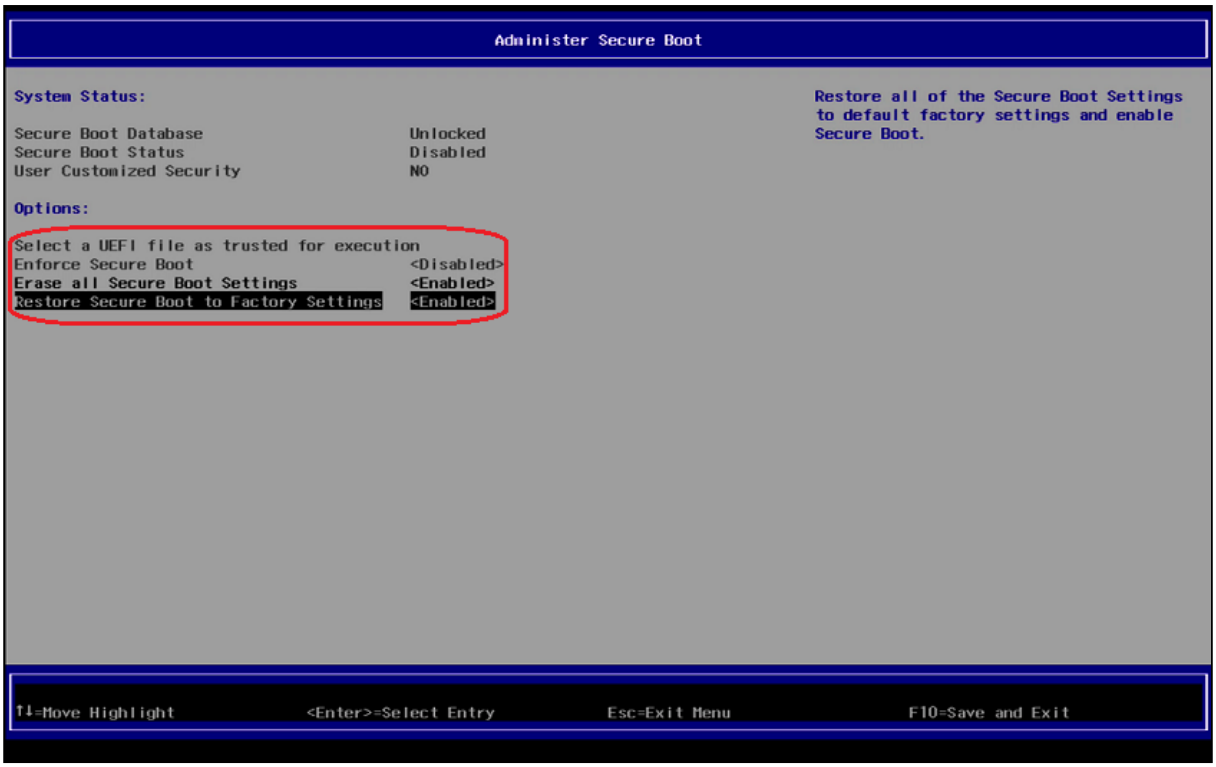
4. In the screen **Administer Secure Boot**, you will find **Erase all Secure Boot Settings** and **Restore Secure Boot to Factory Settings** set to **<Disabled>**.



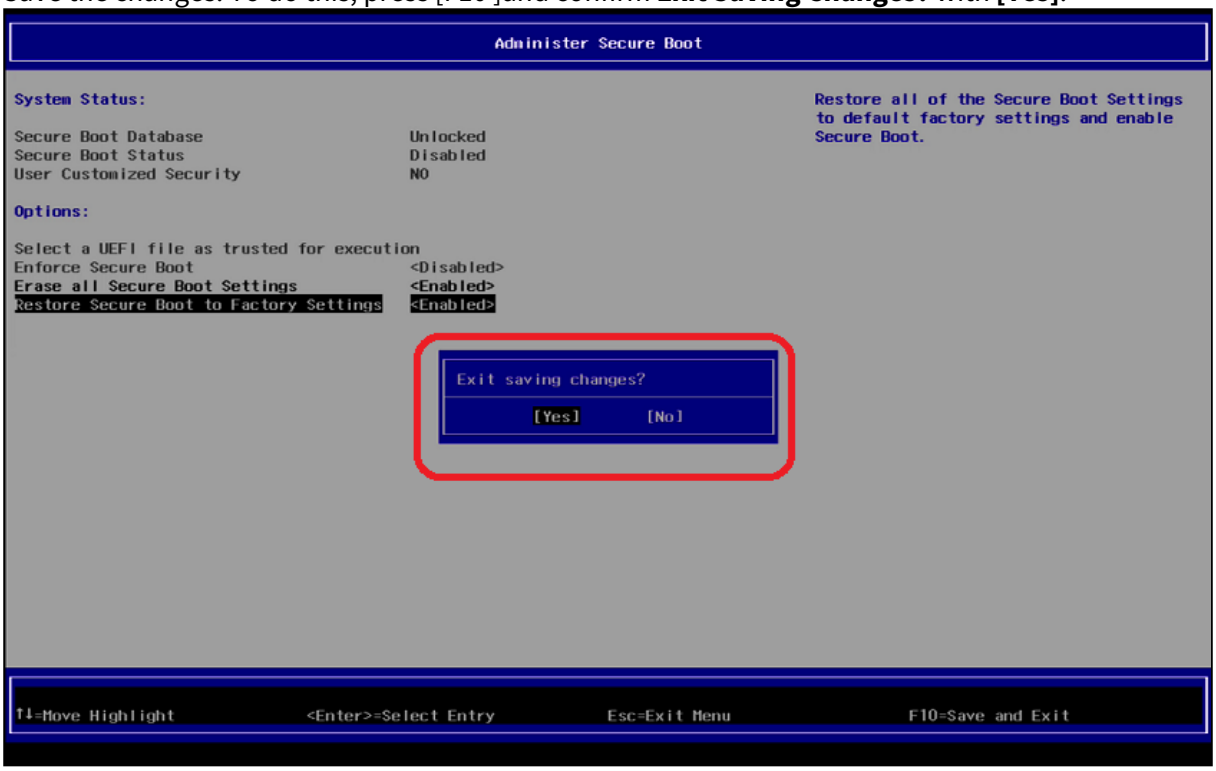
5. In the screen **Administer Secure Boot**, set **Erase all Secure Boot Settings** and **Restore Secure Boot to Factory Settings** to **<Enabled>**.



6. **Erase all Secure Boot Settings** and **Restore Secure Boot to Factory Settings** are now set to **<Enabled>**.
   If **Enforce Secure Boot** is not grayed out as in the picture below, change that option to as well.



7. Save the changes. To do this, press [F10]and confirm **Exit Saving Changes?** with **[Yes]**.



The changes will be saved and the device will be rebooted.

8. As a last step, verify that Secure Boot is working, see Verifying that Secure Boot is Enabled (see page 280) .

Enabling UEFI Secure Boot in UD7-W10 10

Prerequisites

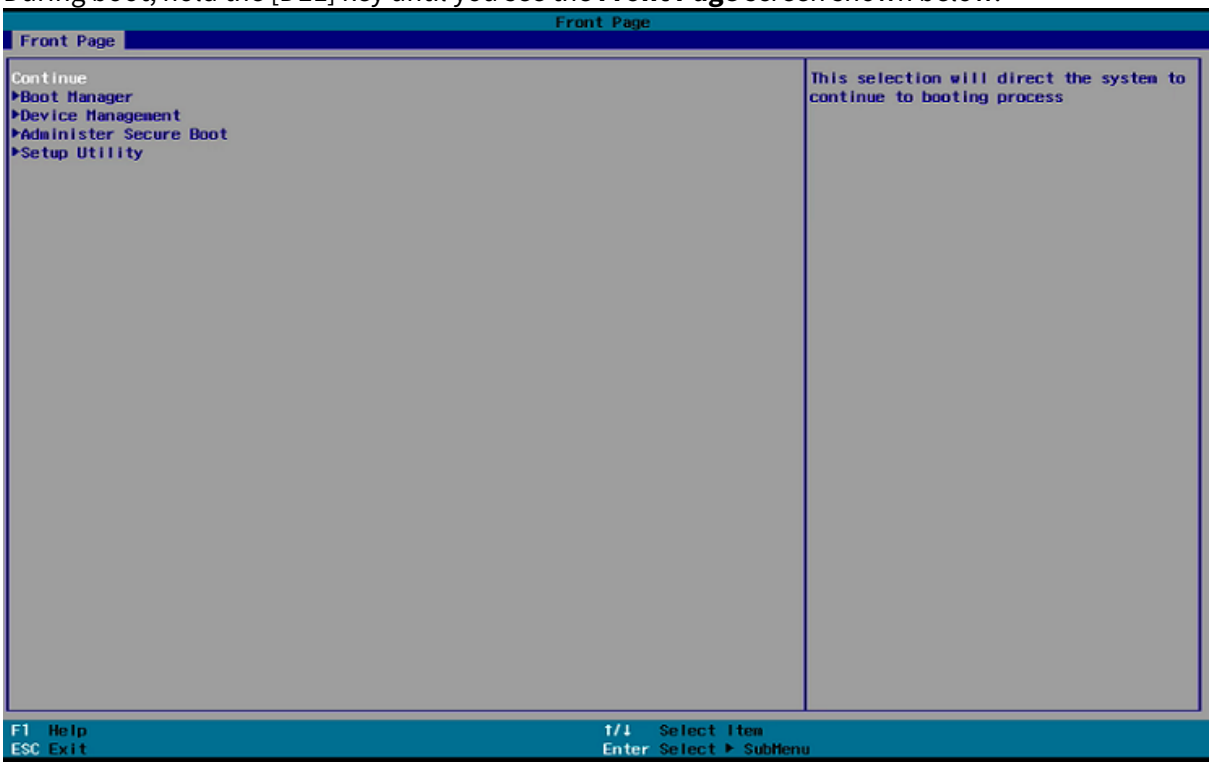
- Microsoft Windows IoT 4.03.100 or higher

UD7-W10 10 supports UEFI Secure Boot by default and no BIOS update is necessary.

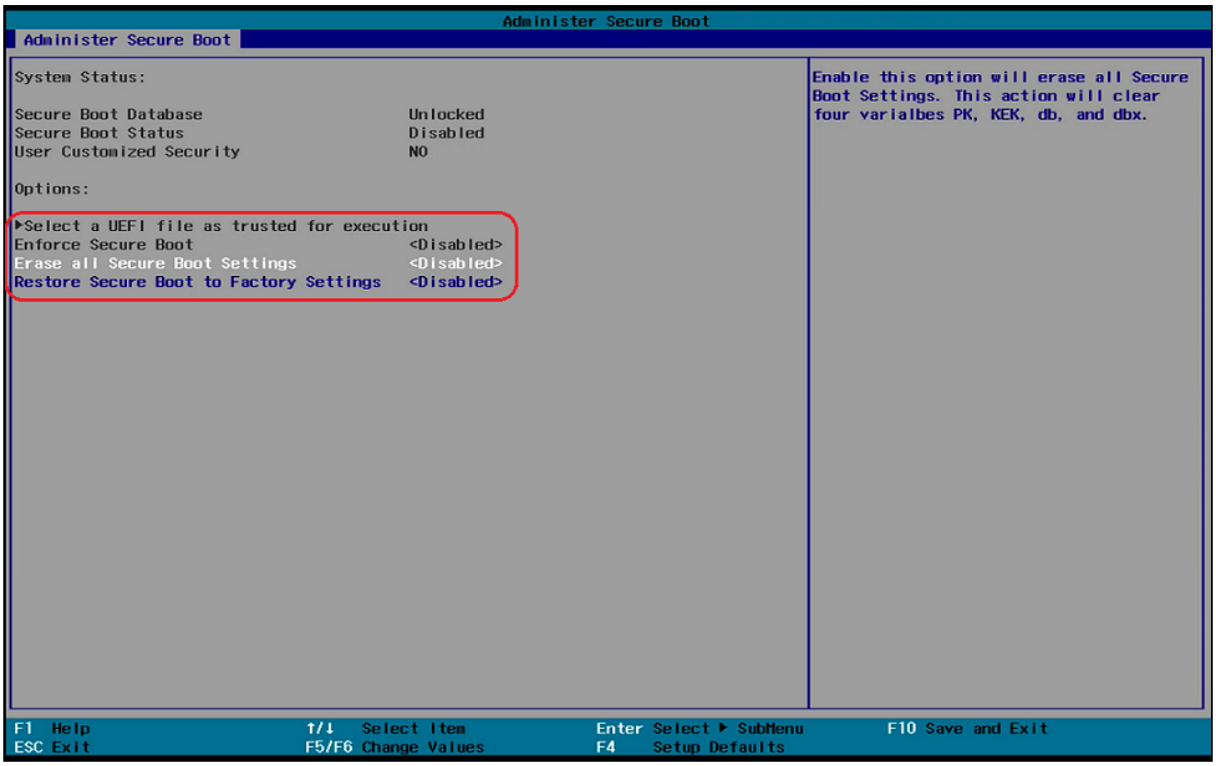
It is crucial to set a BIOS password to prevent users from disabling Secure Boot.

Activating the Secure Boot Feature

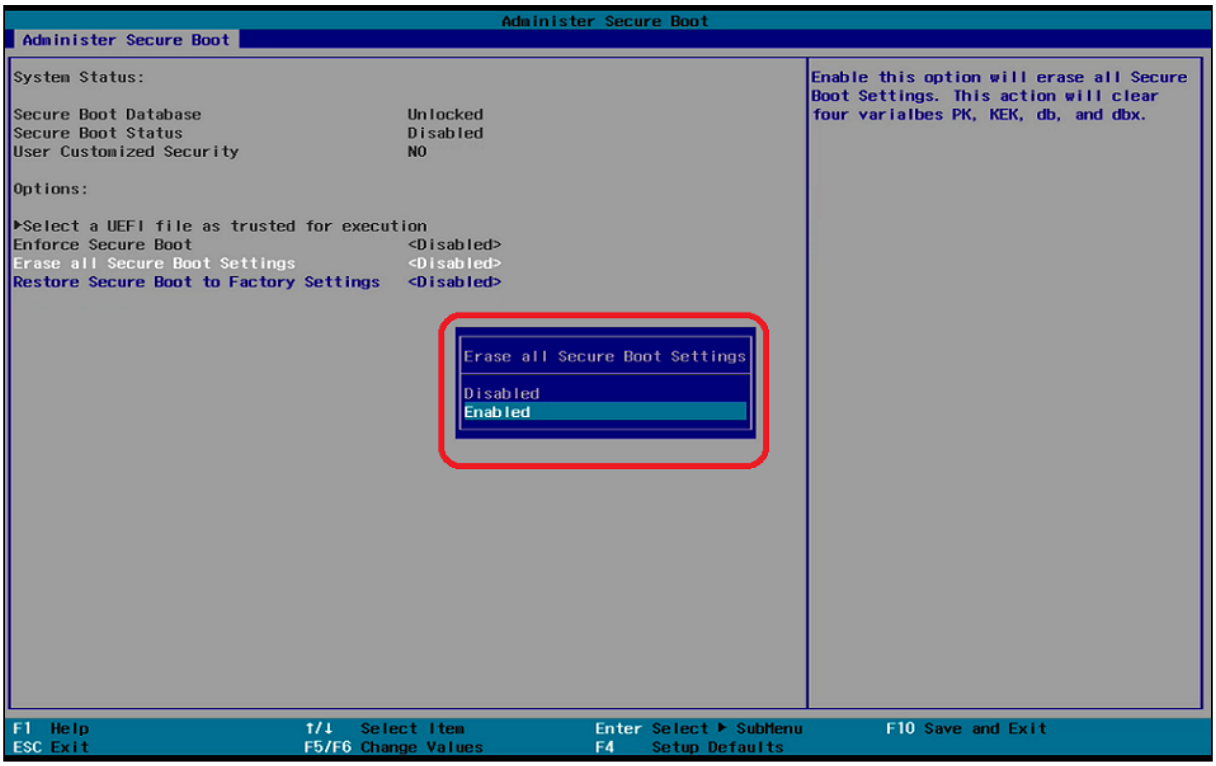
1. Turn on (or restart) the IGEL device.
2. During boot, hold the [DEL] key until you see the **Front Page** screen shown below.



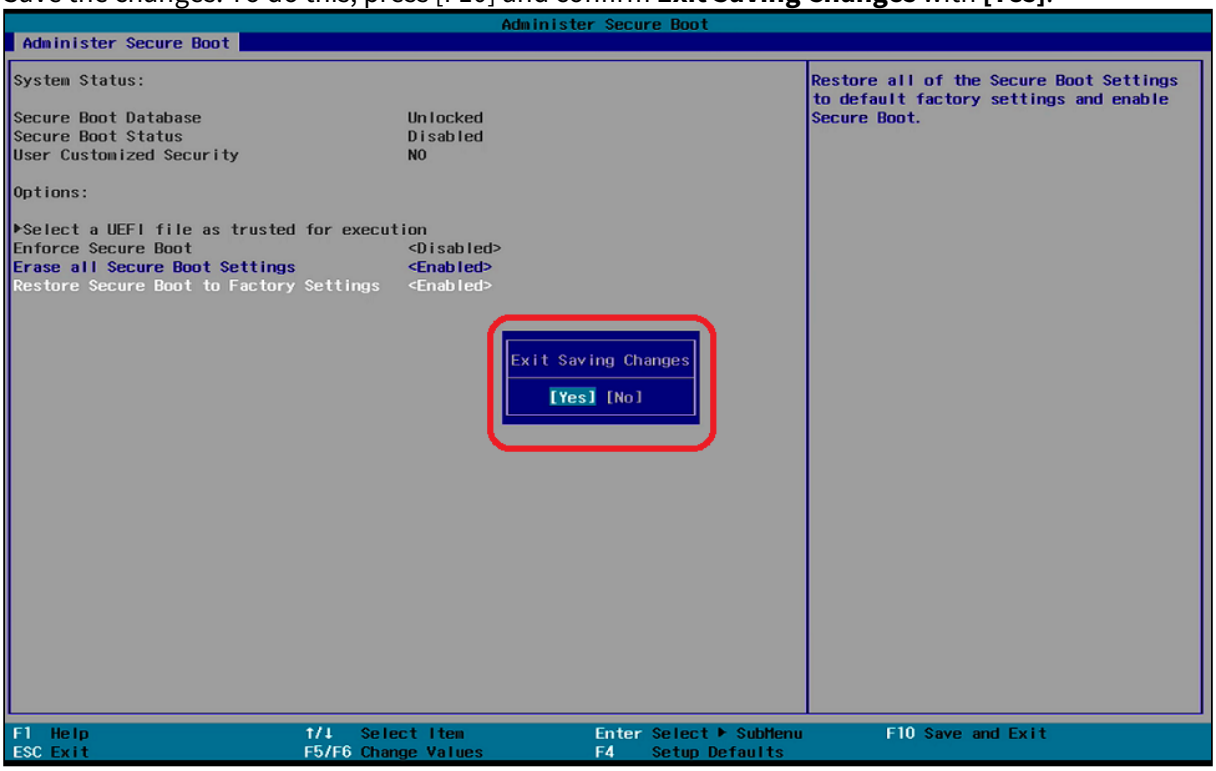
3. In the **Administer Secure Boot** screen, you will find **Erase all Secure Boot Settings** and **Restore Secure Boot to Factory Settings** set to **<Disabled>**.



4. Change both **Erase all Secure Boot Settings** and **Restore Secure Boot to Factory Settings** to **<Enabled>**.
   If **Enforce Secure Boot** is not grayed out as in the picture below, change that option to as well.



5. Save the changes. To do this, press [F10] and confirm **Exit Saving Changes** with **[Yes]**.



The changes will be saved and the device will be rebooted.

6. As a last step, verify that Secure Boot is working, see Verifying that Secure Boot is Enabled (see page 280) .

Verifying that Secure Boot is Enabled

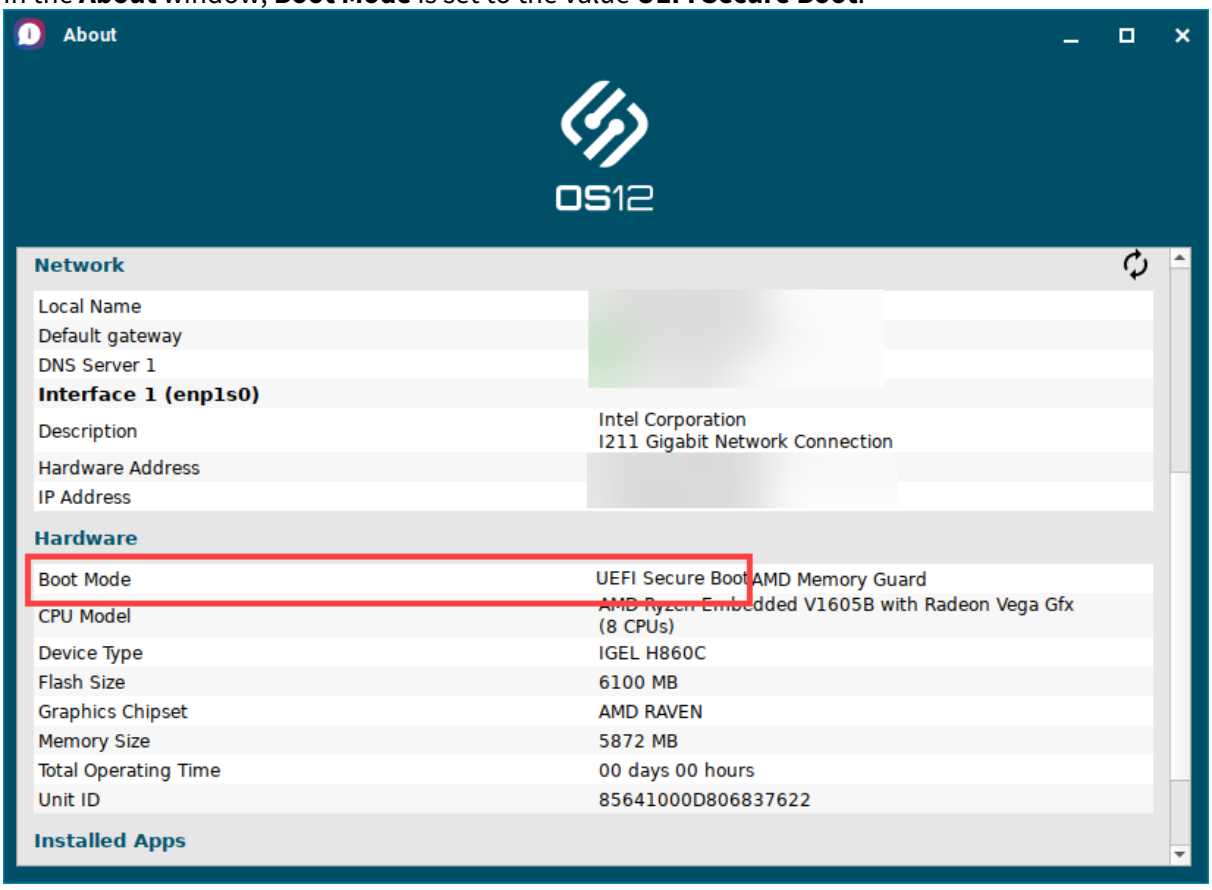
UEFI Secure Boot support is available in IGEL OS 10.04.100 or higher as well as Windows 10 IoT 4.03.100 or higher.

Check the following points to see whether UEFI Secure Boot has been properly enabled.

It is important to verify that UEFI Secure Boot has been properly enabled.

On IGEL OS 12.01 and Higher

- In the **About** window, **Boot Mode** is set to the value **UEFI Secure Boot**.



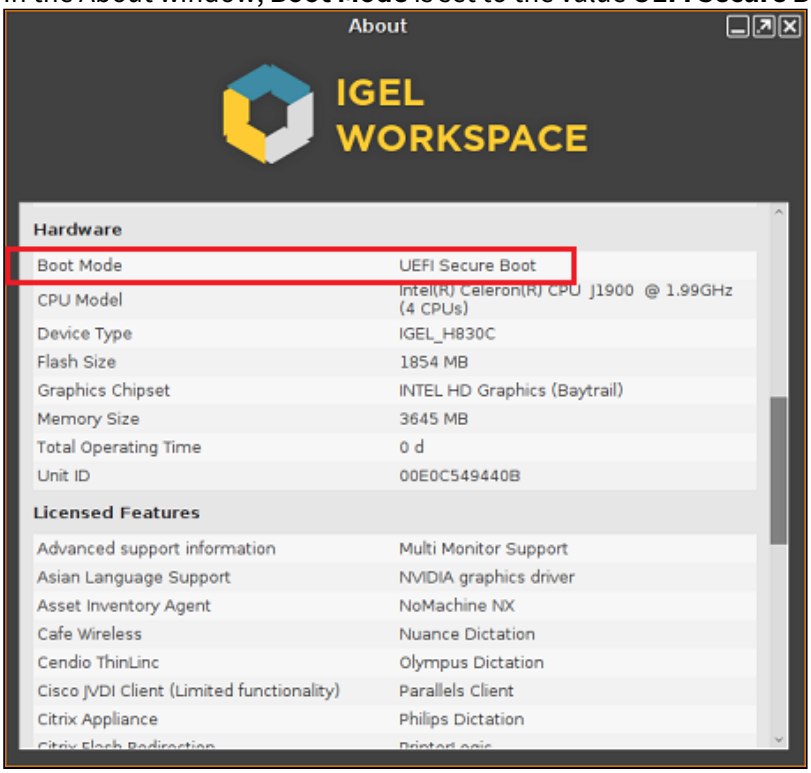
Note that there is a downgrade limit if the secure boot is enabled, see Downgrade Limit on IGEL OS 12.7.1 or Higher[54].

54. https://kb.igel.com/en/igel-os-base-system/current/downgrade-limit-on-igel-os-12-7-1-or-higher

On IGEL OS 11.01.100 and Higher

- The boot splash contains a lock symbol.

- In the About window, **Boot Mode** is set to the value **UEFI Secure Boot**.



On IGEL OS 10.04.100 - 10.05.500

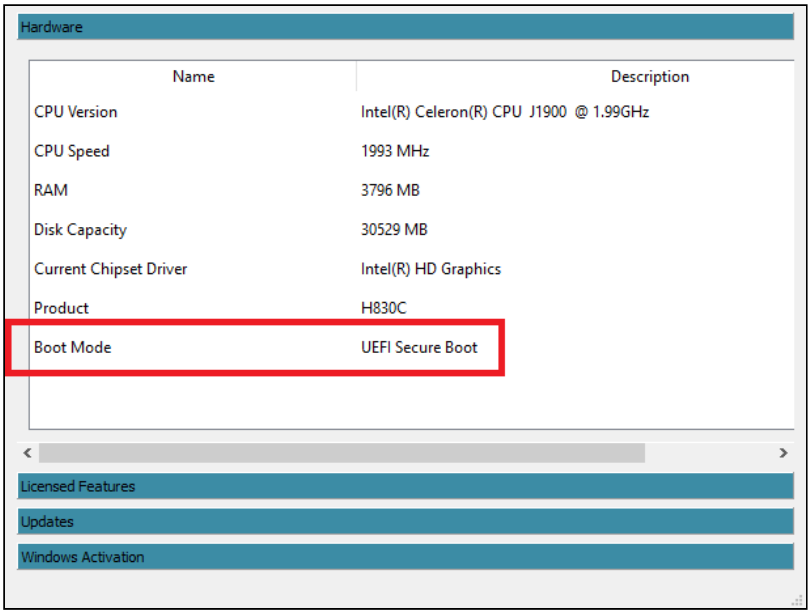
- The boot splash contains a lock symbol.

- In the About window, **Boot Mode** is set to the value **UEFI Secure Boot**.

On Microsoft Windows 10 IoT

- The boot splash contains a lock symbol.

- In the IGEL Device Information tool, in the **Hardware** tab, **Boot Mode** is set to the value **UEFI Secure Boot**.

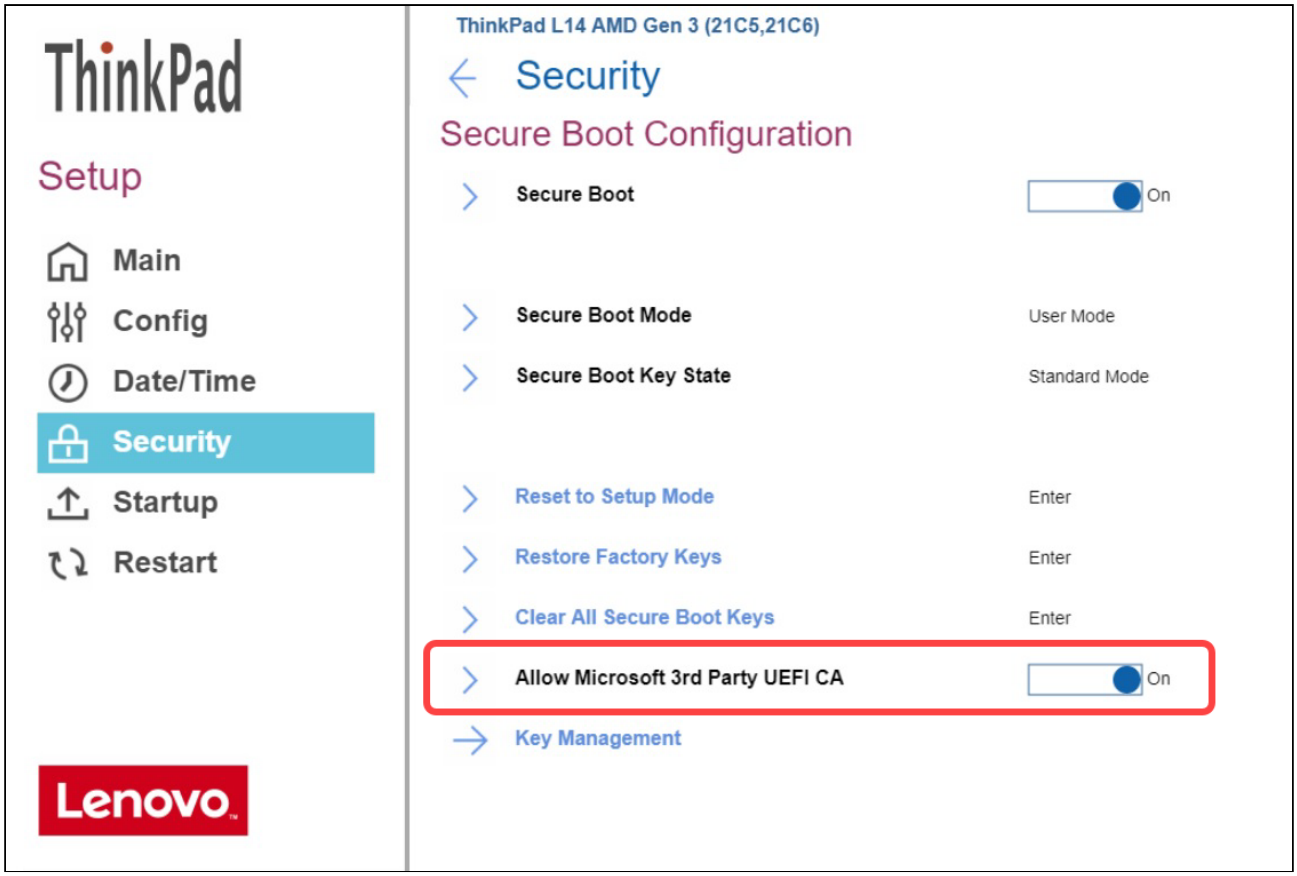


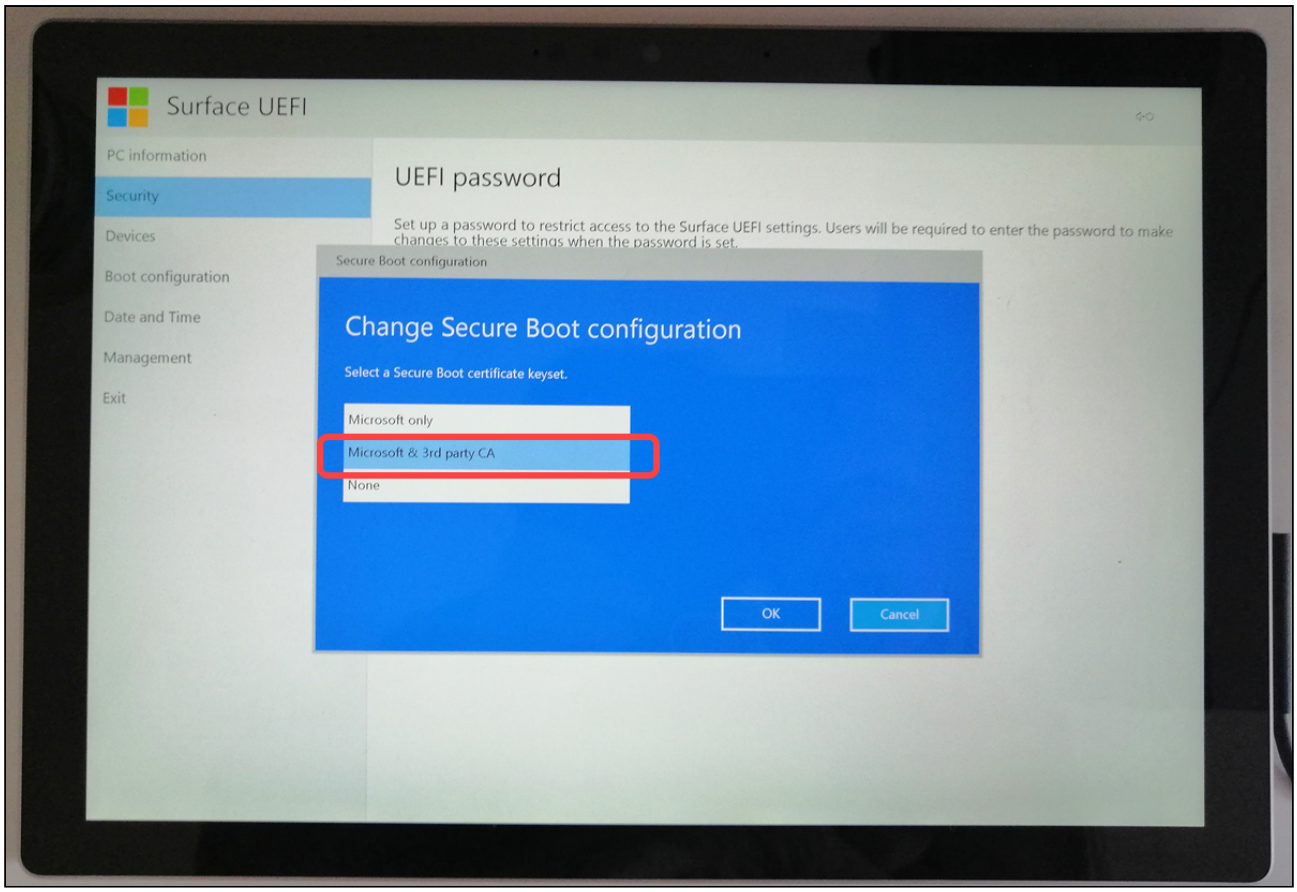
Secured-Core PCs: Microsoft 3rd-Party UEFI Certificate for Secure Boot

On modern computers such as secured-core PCs (see e.g. https://www.microsoft.com/en-us/windows/business/devices?col=secured-core-pcs), there may be a BIOS setting related to Secure Boot that allows the use of Microsoft's 3rd party UEFI Secure Boot Certificate. The usual description of such a BIOS setting is "Allow Microsoft 3rd Party UEFI CA". This setting must be set to enabled, as IGEL uses the 3rd party certificate to support UEFI Secure Boot.

If UEFI Secure Boot is enabled, but "Allow Microsoft 3rd Party UEFI CA" is not enabled, you may be unable to boot IGEL OS Creator or UD Pocket. Similarly, if the setting "Allow Microsoft 3rd Party UEFI CA" is disabled after a previous installation of IGEL OS, IGEL OS will fail to boot.

Examples:




Surface UEFI
PC information
Security
Devices
Boot configuration
Date and Time
Management
Exit
UEFI password
Set up a password to restrict access to the Surface UEFI settings. Users will be required to enter the password to make changes to these settings when the password is set.
Secure Boot configuration
Change Secure Boot configuration
Select a Secure Boot certificate keyset.
Microsoft only
Microsoft & 3rd party CA
None
OK
Cancel

AMD Secure Processor

To enhance the security at the hardware level, IGEL implements the AMD Secure Processor technology. The AMD Secure Processor is a built-in dedicated security system that checks if the BIOS has a valid signature and thus secures the next step in the boot process. This ensures that only devices with a signed BIOS will boot.

For more information about the AMD Secure Processor, visit the AMD website https://www.amd.com/en/technologies/.

IGEL Devices with the Integrated AMD Secure Processor

- *Hardware > Versions of Hardware > (1-en) Hardware > (1-en) UD3 > (1-en) M350C > (1-en) Manual 1 > (1-en) IGEL UD3 M350C: Technical Specification*
- *Hardware > Versions of Hardware > (1-en) Hardware > (1-en) UD7 > (1-en) H860C > (1-en) Manual 2 > (1-en) IGEL UD7 H860C: Technical Specification*
- UD7 Model H850C (see page 287)

UD7 Model H850C

As from December 2019, IGEL UD7 model H850C is equipped with the AMD Secure Processor (see page 286).

> H850C devices manufactured before December 2019 do not include the AMD Secure Processor and cannot be upgraded.

> The implementation of the AMD Secure Processor technology required mainboard and UEFI modification; backward compatibility is not supported.

> The AMD Secure Processor technology increases the system boot time between 3 and 4.5 seconds.

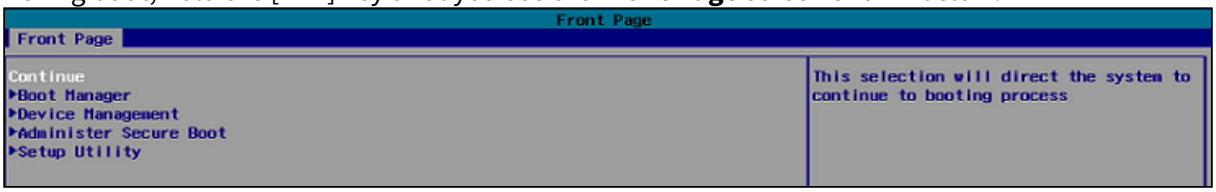
Features Distinguishing H850C Devices with the AMD Secure Processor

The following features distinguish H850C devices with the integrated AMD Secure Processor from H850C devices without it:

- BIOS version 3.9.13-10092019 and higher

How to find out your BIOS version...

1. Turn on (or restart) your UD7 device.
2. During boot, hold the [DEL] key until you see the **Front Page** screen shown below.



3. Choose **Setup Utility**.
   The **InsydeH20 Setup Utility** opens.
4. Press [F9] to open the **System Information** window.
5. In the **System Information** window, check **BIOS Version**.

- Hardware ID "LX-11", introduced with IGEL OS version 11.03.
- A black dot in the right bottom corner of the device label, which you can see if you pull out the black label holder located at the rear of the device:


www.igel.com
Thin Client 精簡型電腦
產品型號(Model Name): IGEL-H850C
輸入規格 (Input Rating): +12V⎓5A
製造商(Manufacturer): IGEL Technology GmbH
地址(Address):Hanna-Kunath-Str.31
28199 Bremen, Germany
Use only power supplies listed in the user manual.
CAN ICES-3(B)/NMB-3(B)
Made in China 中國製造 Designed in Germany 德國設計
LISTED
E308119
R3A044
RoHS

AMD Memory Guard

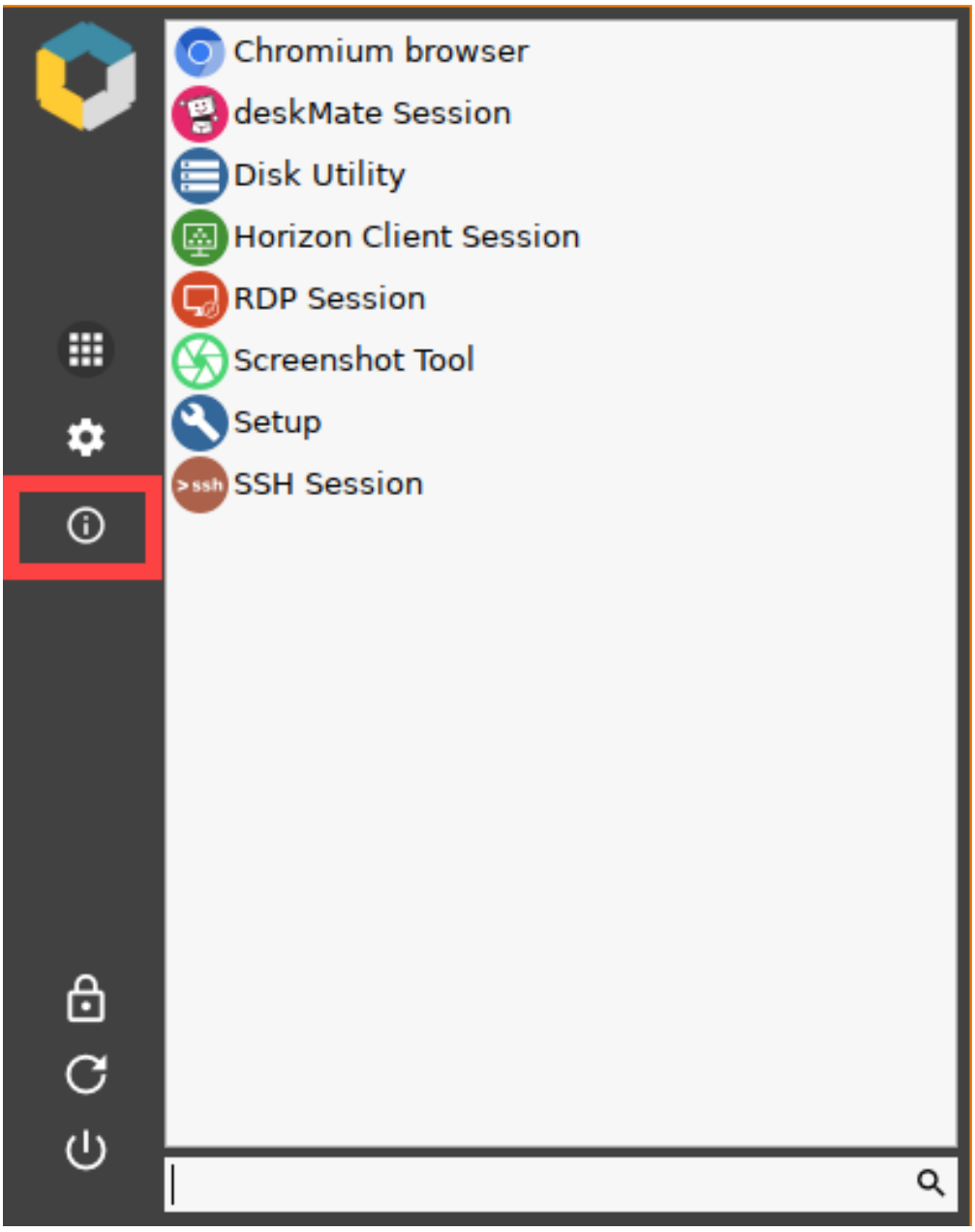
With AMD Memory Guard, IGEL enhances the security capabilities of the *Hardware > UD3 > M350C > Manual of UD3 M350C > IGEL UD3 M350C: Technical Specification* and *Hardware > UD7 > H860C > Manual of UD7 H860C > IGEL UD7 H860C: Technical Specification*.

AMD Memory Guard enables real-time memory encryption, which helps to protect against physical attacks and to secure data stored in RAM. The encryption is done on the basis of the randomly generated AES 128-bit encryption key and performed as such by the AMD Secure Processor (see page 286) integrated in the IGEL device.

For more information about AMD Memory Guard, see https://www.amd.com/system/files/documents/amd-memory-guard-white-paper.pdf.

Activation / Deactivation

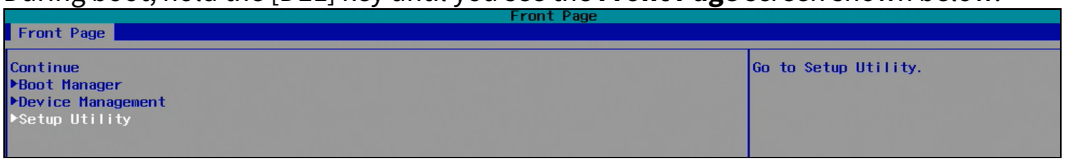
- AMD Memory Guard is available and activated by default as of BIOS version 3.5.13A-07222020.
- The activation/deactivation status is indicated in the **About** window, accessible via the icon  , as of IGEL OS 11.04.100.



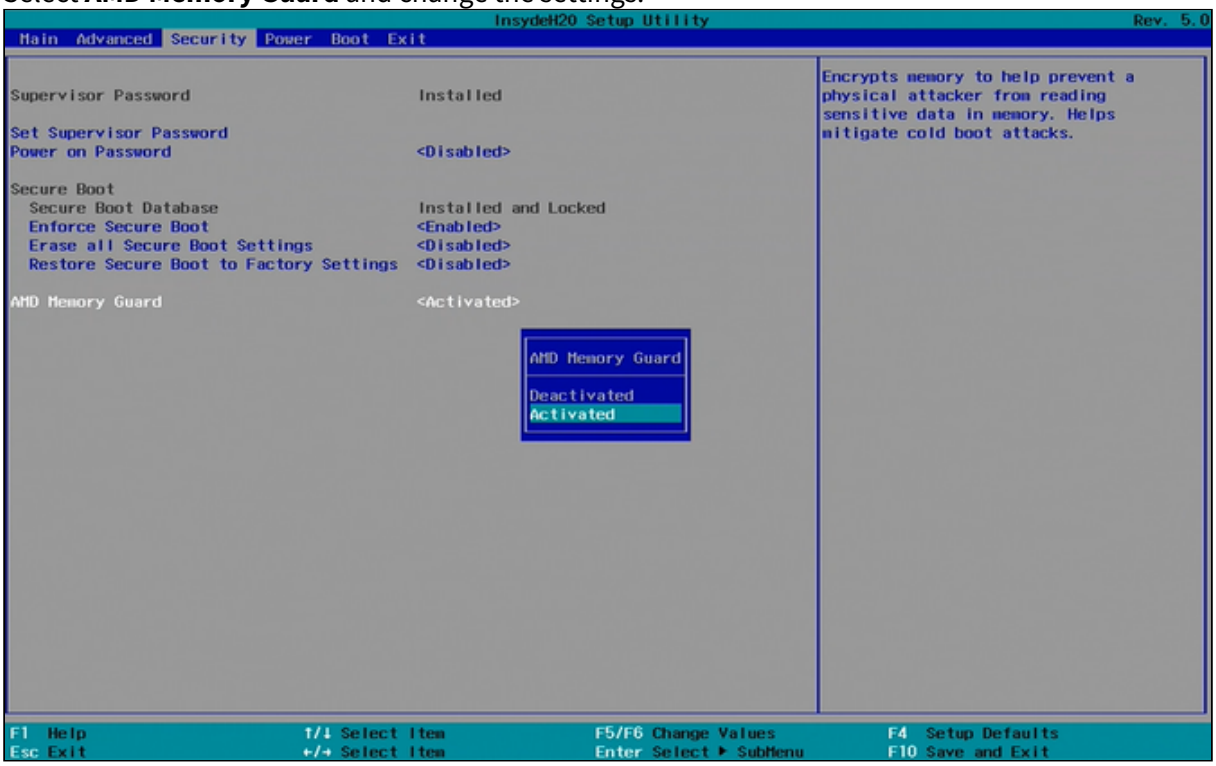
- AMD Memory Guard can be deactivated in BIOS under **Setup Utility > Security**.

How to deactivate AMD Memory Guard

1. Turn on (or restart) your device.
2. During boot, hold the [DEL] key until you see the **Front Page** screen shown below.



3. Choose **Setup Utility**.
   The **InsydeH20 Setup Utility** opens.
4. Go to **Security**.
5. Select **AMD Memory Guard** and change the settings.



6. Press [F10] to save the changes.

As AMD Memory Guard has only a minor impact on system performance – e.g. on M350C, the reduction equals to 1-1.5% – it is advisable to leave the feature activated.

BSI Grundschutz

Anleitung zum IT-Grundschutz-konformen Betrieb von IGEL OS 11.03.100

Über dieses Dokument

Dieses Dokument beschreibt, welche Einstellungen an einer IGEL OS Installation vorgenommen werden müssen, um die Sicherheitsziele aus dem IT-Grundschutz OPS.1.2.4.A2 „Sicherheitstechnische Anforderungen an den Telearbeitsrechner“ zu erreichen. Es stützt sich auf die IT-Grundschutz-Komponenten OPS.1.2.4.M2 „Sicherheitstechnische Anforderungen an den Telearbeitsrechner“, SYS.2.1 „Allgemeiner Client“ und SYS.2.3 „Clients unter Unix“.

Diese Version des Dokuments gilt für IGEL OS 11.03.100.

Grundsätzliche Vorgaben zur Administration

Administration mittels UMS

Im IT-Grundschutz-konformen Betrieb darf IGEL OS ausschließlich mittels der IGEL Universal Management Suite (UMS) in Version 6.03.130 oder neuer fernadministriert und konfiguriert werden. So entsteht ein vollständiges Protokoll der administrativen Tätigkeiten und Konfigurationsänderungen in der Datenbank der UMS.

Um ein vollständiges Protokoll zu haben, muss die Protokollierung erst in der UMS Konsole unter **UMS Administration > Globale Konfiguration > Logging** aktiviert werden, siehe Logging in the IGEL UMS[55]. Beachten Sie auch Logging-Einstellungen unter **UMS Administration > Globale Konfiguration > Fernzugriff**.

Kein lokales Setup nutzen

Das lokale Setup-Tool auf dem Gerät darf nicht benutzt werden. Ist im Folgenden „Setup“ erwähnt, so ist der Setup-Dialog innerhalb der UMS gemeint.

Kein lokales Terminal nutzen

Das lokale Terminal auf dem Gerät darf nicht benutzt werden.

55. https://kb.igel.com/en/universal-management-suite/current/logging-in-the-igel-ums

Fernwartung

Anforderung

Wenn der Telearbeitsrechner über Fernwartung (Remote Administration) administriert werden sollte, ist sicherzustellen, dass die Fernadministration nur autorisiert durchgeführt werden kann. Bei der Fernwartung müssen eine Authentisierung des Fernwartungspersonals, die Verschlüsselung der übertragenen Daten und eine Protokollierung der Administrationsvorgänge gewährleistet sein.

Maßnahme: In Universal Management Suite (UMS) registrieren

Das Gerät muss in der Universal Management Suite registriert und darüber fernadministriert werden.

1. Klicken Sie in der UMS Konsole das Symbol
   
   (Geräte scannen).
2. Klicken Sie **Suchen**.
   Die Ergebnisliste wird angezeigt.
3. Geben Sie im Feld **Filter** die MAC-Adresse des gewünschten Geräts ein, um es zu finden.
   Das gesuchte Gerät wird angezeigt.
4. Aktivieren Sie die Checkbox **Aufnehmen** im Eintrag des Geräts und klicken Sie **OK**.
   Das Gerät wird registriert und lässt sich nun mittels Universal Management Suite fernadministrieren.

Anmerkungen

Nach seiner Registrierung lässt sich das Gerät nur noch von dieser UMS-Instanz fernadministrieren, die sich durch ihr TLS-Zertifikat ausweist.

Die Kommunikation erfolgt transportverschlüsselt mit TLSv1.2.

Maßnahme: Secure Shadowing aktivieren

Auf dem Gerät muss Secure Shadowing aktiviert werden.

1. Gehen Sie im Setup zu **System > Fernzugriff > Spiegeln**.
2. Aktivieren Sie die Checkbox **Spiegeln des Desktops mit VNC erlauben**.
3. Aktivieren Sie die Checkbox **Sichere Verbindung**.
4. Klicken Sie **Übernehmen**.

Anmerkung

Bei aktiviertem Secure Shadowing kann ausschließlich via Universal Management Suite von berechtigten Nutzern eine VNC-Verbindung zum Gerät aufgebaut werden. Die Verbindung ist transportverschlüsselt mit TLSv1.2., und die

VNC-Sitzungen werden protokolliert. In der UMS Konsole sind diese Protokolle unter **System > Logging > Fernzugriffe** einsehbar.

Zugriffskontrolle

Anforderungen

Telearbeitsrechner dürfen nur von autorisierten Personen benutzt werden. Damit wird sichergestellt, dass nur autorisierte Personen auf Daten und Programme zugreifen können, die auf einem Telearbeitsrechner gespeichert sind. Gleiches gilt für Informationen und Daten, die über den Telearbeitsrechner erreichbar wären (zum Beispiel mittels VPN). Autorisierte Personen sind der Administrator des Telearbeitsrechners und der Telearbeiter nebst seinem Stellvertreter.

Der Telearbeitsrechner muss über einen Identifizierungs- und Authentisierungsmechanismus verfügen.

Maßnahme: Passwort für lokalen Administrator setzen

Für das lokale Administrator-Konto muss ein Passwort gesetzt sein.

Anmerkung: Dadurch wird auch der Zugriff auf den lokalen Terminalemulator und die Setup-Anwendung für den normalen Benutzer gesperrt.

1. Gehen Sie im IGEL Setup zu **Sicherheit > Passwort**.
2. Aktivieren sie im Bereich Administrator die Checkbox **Passwort verwenden**.
3. Sobald sie aufgefordert werden, geben Sie das Passwort zwei Mal ein.
4. Klicken Sie **Übernehmen**.

Maßnahme: Active-Directory-Login für Benutzer konfigurieren

Für das Benutzer-Konto muss die Anmeldung via Active Directory eingestellt sein.

1. Gehen Sie im IGEL Setup zu **Sicherheit > Active Directory/Kerberos**.
2. Aktivieren Sie die Checkbox.
3. Tragen Sie die **Standarddomäne (vollständiger Domänenname)** ein.
4. Klicken Sie **Übernehmen**.
5. Gehen Sie im IGEL Setup zu **Sicherheit > Active Directory/Kerberos > Domäne 1**
6. Klicken Sie das Plus-Zeichen, um einen neuen Eintrag zu erstellen.
7. Geben Sie bei **Domänencontroller** den Namen oder die IP-Adresse des Domänencontrollers (Kerberos Key Distribution Center) ein. Eine Portnummer kann an den Hostnamen angehängt werden; der Portnummer muss ein Doppelpunkt vorangestellt werden.
8. Klicken Sie **Weiter**.
   Der Domänencontroller wird in der Liste der Domänencontroller eingefügt.
9. Gehen Sie im IGEL Setup zu **Sicherheit > Anmeldung > Active Directory/Kerberos**.
10. Aktivieren Sie die Checkbox **Anmeldung an Active-Directory Domäne**.
11. Aktivieren Sie die Checkbox **Verknüpfung zum Abmelden: Startmenü**.
12. Klicken Sie **Übernehmen**.

Der Benutzer muss eine Möglichkeit haben, sein Passwort zu ändern.

1. Gehen Sie im IGEL Setup zu **Zubehör > Passwort ändern >Passwort ändern**.
2. Aktivieren Sie die Checkbox

3. Klicken Sie **Übernehmen**.
   Der Benutzer findet nun in der Schnellstartleiste ein Schlüssel-Icon, das den Dialog zur Passwortänderung öffnet.

Anmerkung: Passwortkomplexität

Anforderungen an die Komplexität des Benutzerpassworts müssen im Active Directory definiert werden. Dazu ist die Dokumentation von Microsoft zu konsultieren, etwa https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc770394(v=ws.10)

Maßnahme: Automatische Bildschirmsperre aktivieren

Es muss die Bildschirmsperre aktiviert werden, die den Bildschirm nach einer Zeitspanne der Inaktivität von Maus und Tastatur sperrt. Zum Entsperren muss sich der Benutzer mit seinem Passwort authentisieren.

1. Gehen Sie im IGEL Setup zu **Benutzeroberfläche > Bildschirmsperre/-schoner**.
2. Wählen Sie bei **Passwortschutz** den Eintrag **Benutzer**.
3. Aktivieren sie die Checkbox **Hotkey**.
4. Wählen Sie bei **Steuertasten** die Option **Win**.
5. Geben Sie bei **Taste** ein l (kleines L wie in „lock“) ein.
6. Aktivieren sie die Checkbox **Autostart**.
7. Gehen Sie zu **Optionen**.
8. Wählen Sie bei **Passwort für Bildschirmsperre** die Option **Benutzerpasswort**.
9. Klicken Sie **Übernehmen**.

Die Bildschirmsperre tritt standardmäßig nach 5 Minuten Inaktivität ein. Weitere Einstellungsmöglichkeiten sind im IGEL OS-Handbuch zu finden.

Absicherung des Bootvorgangs

Anforderung

Der Telearbeitsrechner sollte über einen Boot-Schutz verfügen, um zu verhindern, dass unbefugt von Wechseldatenträgern gebootet werden kann.

Maßnahme: USB-Boot deaktivieren

Auf IGEL UD-LX-Geräten

USB Boot muss im UEFI deaktiviert sein. Das Booten von USB-Medien ist im Auslieferungszustand bereits deaktiviert. Um es im Bedarfsfall zu deaktivieren, führen Sie folgende Schritte aus.

1. Halten Sie die Entfernen-Taste gedrückt, während das System bootet.
   Das UEFI-Menü öffnet sich.
2. Verwenden Sie die Pfeil-Tasten und die Return-Taste, um **SCU** auszuwählen.
   Das **Setup Utility** öffnet sich.
3. Gehen Sie zu **Boot**.
4. Setzen Sie **USB Boot** auf **Disabled**.
5. Drücken Sie **F10**
6. Bestätigen Sie die Nachfrage **Exit Saving Changes?**
   Das Gerät bootet neu.

Auf Geräten von Drittherstellern

Deaktivieren Sie das Booten von USB-Medien nach der Anleitung Ihres UEFI-Herstellers.

Maßnahme: UEFI-Passwort setzen

Auf IGEL UD-LX-Geräten

1. Halten Sie die **Entfernen**-Taste gedrückt, während das System bootet.
   Das UEFI-Menü öffnet sich.
2. Verwenden Sie die Pfeil-Tasten und die **Return**-Taste, um **SCU** auszuwählen.
   Das **Setup Utility** öffnet sich.
3. Gehen Sie zu **Security**.
4. Wählen Sie **Set Supervisor Password** aus.
5. Drücken Sie **Return**.
6. Geben Sie das gewünschte UEFI-Passwort ein und drücken Sie **Return**.
7. Wiederholen Sie die Eingabe des UEFI-Passworts und drücken Sie zwei Mal **Return**.
8. Drücken Sie **F10**.
9. Bestätigen Sie die Nachfrage **Exit Saving Changes?**
   Das Gerät bootet neu.

Auf Geräten von Drittherstellern

Setzen Sie ein UEFI-Passwort nach der Anleitung Ihres UEFI-Herstellers.

Maßnahme: Gerät mit UEFI Secure Boot benutzen

Zum Betrieb von IGEL OS muss ein Gerät verwendet werden, das UEFI Secure Boot unterstützt.

Das ist der Fall bei allen IGEL UD-LX-Geräten.

Maßnahme: UEFI Secure Boot aktivieren

Auf IGEL UD-LX-Geräten

Auf allen IGEL UD-LX-Geräten, die seit dem 15. April 2019 ausgeliefert wurden, ist UEFI Secure Boot bereits aktiviert. Um UEFI Secure Boot zu einem späteren Zeitpunkt wieder zu aktivieren, folgen Sie den **UEFI Secure Boot Enabling Guides** unter https://wiki.test.toolchain.igel.kreuzwerker.net/securitysafety/uefi-secure-boot-enabling-guides-2271735.html

Auf Geräten von Drittherstellern

Aktivieren Sie UEFI Secure Boot nach der Anleitung Ihres UEFI-Herstellers.

Schutz bei Diebstahl oder Defekt

Anforderungen

Schäden aufgrund eines Diebstahls oder Defektes eines Telearbeitsrechners müssen tolerabel sein. Telearbeitsrechner werden üblicherweise in einer wenig gesicherten Umgebung eingesetzt, sodass ein Diebstahl oder Defekt wahrscheinlicher ist als in der geschützten Betriebsumgebung einer Institution. Darunter kann nicht nur die Verfügbarkeit, sondern auch die Vertraulichkeit der gespeicherten Daten leiden. Um die Schäden bei Diebstählen gering zu halten, sollten die Daten zum Beispiel nur verschlüsselt gespeichert werden. Um Schäden durch Defekte zu begrenzen, eignen sich zum Beispiel regelmäßig durchgeführte Datensicherungen.

Maßnahmen

- Es dürfen keine Passwörter für Dienste in den Einstellungen des Geräts gespeichert werden.
- Es dürfen keine privaten Schlüssel ohne Passphrase auf dem Massenspeicher des Geräts gespeichert werden.
- Es dürfen keine Nutzdaten auf dem Massenspeicher des Geräts gespeichert werden.

Schutz vor Manipulation

Anforderungen

Telearbeiter sollten wenigstens offensichtliche versuchte oder erfolgte Manipulationen am Telearbeitsrechner erkennen können. Damit wird sichergestellt, dass der Telearbeitsrechner in einem integren Zustand verbleibt, auch wenn Manipulationsversuche nicht ausgeschlossen sind.

Anmerkung

Kryptografisch signierte Betriebssystem- und Software-Partitionen auf dem Massenspeicher schützen IGEL OS ab 11.03.100 vor Manipulation. Beim Systemstart und während des Betriebs überprüft IGEL OS anhand dieser Signaturen die Integrität und Authentizität der Partitionen.

- Wird eine veränderte Software-Partition (optionale Software) festgestellt, wird im Verbose-Boot-Modus die Meldung „Invalid signature - Failed to read partition <name>“ angezeigt. Das System startet zur Behebung automatisch einen Update-Vorgang, um von der konfigurierten Firmware-Quelle eine integre und authentische Partition herunterzuladen. Scheitert dies, wird eine Desktop-Meldung angezeigt.
- Wird eine veränderte Betriebssystem-Partition festgestellt, wird im Verbose-Boot-Modus die Meldung „Invalid signature, failed to read critical partition – An firmware update or reinstallation may be required“ angezeigt. In diesem Fall ist eine Neuinstallation des Betriebssystems per IGEL OS Creator 11.03.100 erforderlich. Bei Schwierigkeiten mit dem Bootvorgang, empfiehlt es sich, unbedingt den Verbose Boot-Modus zu verwenden.

Die zur Laufzeit beschreibbaren Daten-Partitionen, darunter `/wfs`, sind verschlüsselt. Dadurch entsteht ebenfalls ein Integritätsschutz, da eine Manipulation im ausgeschalteten Zustand einen Fehler beim Entschlüsseln im Betrieb verursachen würde. Dadurch und durch geeignete Linux-Berechtigungen sind die Konfigurationsdateien in `/wfs` vor Manipulation durch andere User als Root geschützt.

Einschränken der Benutzerumgebung

Anforderung

Es sollte möglich sein, die Benutzerumgebung des Telearbeitsrechners einzuschränken. Damit soll der Administrator festlegen können, welche Programme der Telearbeiter ausführen kann, welche Peripheriegeräte nutzbar sind und welche Änderungen der Telearbeiter am System vornehmen darf. Darüber hinaus sollte der Telearbeiter Einstellungen, die für den sicheren Betrieb notwendig sind, nicht unautorisiert ändern und nicht unerlaubt Fremdsoftware aufspielen können.

Maßnahme: Zugriff auf die virtuellen Linux-Konsolen sperren

1. Gehen Sie im **IGEL Setup** zu **Benutzeroberfläche > Bildschirm > Zugriffskontrolle**.
2. Aktivieren Sie **Konsolenzugriff abschalten**.
3. Klicken Sie **Übernehmen**.

Maßnahme: TCP-Konnektivität des X-Servers deaktivieren

Sofern keine X-Server-Anmeldung über das Netzwerk am Gerät erforderlich ist, muss die TCP-Konnektivität des X-Servers deaktiviert sein. Standardmäßig ist sie auf IGEL OS bereits deaktiviert, doch sollten Sie sie deaktivieren müssen, führen Sie folgende Schritte aus:

1. Gehen Sie im Setup zu **Benutzeroberfläche > Bildschirm > Zugriffskontrolle**.
2. Aktivieren Sie die Checkbox **TCP-Verbindungen deaktivieren**.
3. Klicken Sie **Übernehmen**.

Maßnahme: PC/SC-Dämon entfernen

Der PC/SC-Dämon muss entfernt werden, sofern er nicht für den Einsatz von Smartcards am Arbeitsplatz erforderlich ist.

1. Gehen Sie im Setup zu **Sicherheit > Smartcard > Dienste**
2. Deaktivieren Sie die Checkbox **PC/SC-Dämon aktivieren**.
3. Klicken Sie **Übernehmen**.

Maßnahme: Webbrowser entfernen

Sofern der Webbrowser nicht für den Arbeitsplatz unverzichtbar ist, muss er entfernt werden.

1. Gehen Sie im Setup zu **System > Firmwareanpassung > Features**.
2. Entfernen Sie das Häkchen aus der Checkbox für **Lokaler Internetbrowser (Firefox).**
3. Klicken Sie **Übernehmen**.

Maßnahme: Nicht benötigte Feature-Partitionen entfernen

Alle Feature-Partitionen, die nicht für den Betrieb des Arbeitsplatzes benötigt werden, müssen entfernt werden.

1. Gehen Sie im Setup zu **System > Firmwareanpassung > Features**
2. Deaktivieren Sie die Checkboxen vor sämtlichen Features, außer jenen, die Sie bestimmt brauchen (beispielsweise RDP, falls Sie RDP einsetzen)
   Daneben lassen Sie folgende Features aktiviert:
   - **BIONIC Kompatibilitätsunterstützung**
   - **Fluendo GStreamer Codec-Plugins**
   - **Fluendo GStreamer AAC Decoder**
   - **Hardware-Videobeschleunigung**
   - **NVIDIA Grafiktreiber**
   - **VNC Viewer**
   - **X32-Kompatibilitätsunterstützung**
3. Klicken Sie **Übernehmen**.

Protokollierung und Protokollauswertung

Anforderungen

Telearbeitsrechner sollten über eine Protokollierung und eine Protokollauswertung verfügen.

Anmerkung

IGEL empfiehlt, die Protokollierung im Standardumfang (Authentisierung, Kernel und Daemons) aktiviert zu lassen und die gewünschten Parameter durch Filtern bei der Auswertung einzugrenzen.

Maßnahme: Protokolle an Log-Analyzer weiterleiten

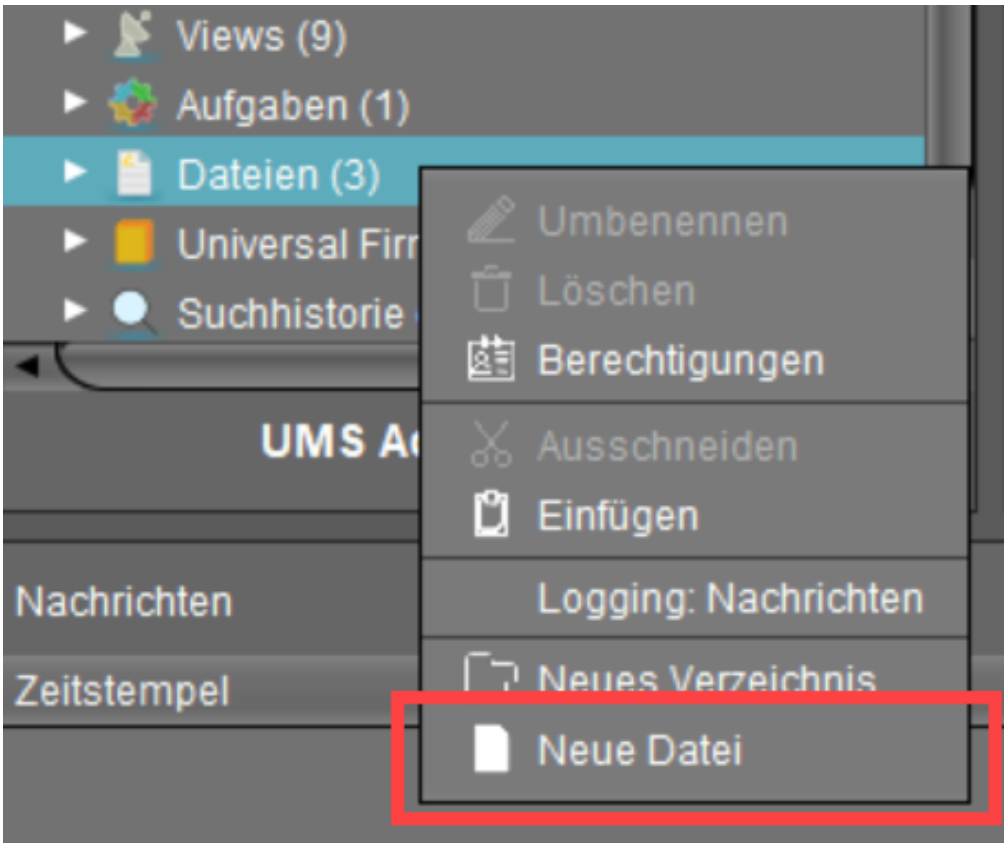
Verwenden Sie einen Log-Collector und -Analyzer, der die Archivierung und das Auswerten von Protokollen nach vielen Gesichtspunkten erlaubt, wie beispielsweise Graylog, Splunk oder den Elastic-Logstash-Kibana-Stack (ELK). Deren Auswertefunktion muss nach den bei der Protokollierung geforderten Datenarten unterscheiden können (zum Beispiel Filtern aller unberechtigten Zugriffe auf alle Ressourcen in einem vorgegebenen Zeitraum). Die Auswertefunktion muss auswertbare (lesbare) Berichte erzeugen, sodass keine sicherheitskritischen Aktivitäten übersehen werden.

Derartige Lösungen können Protokolldaten per Rsyslog-Schnittstelle mit TLS-Verschlüsselung entgegennehmen. Konfigurieren Sie die Weiterleitung durch IGEL OS folgendermaßen:

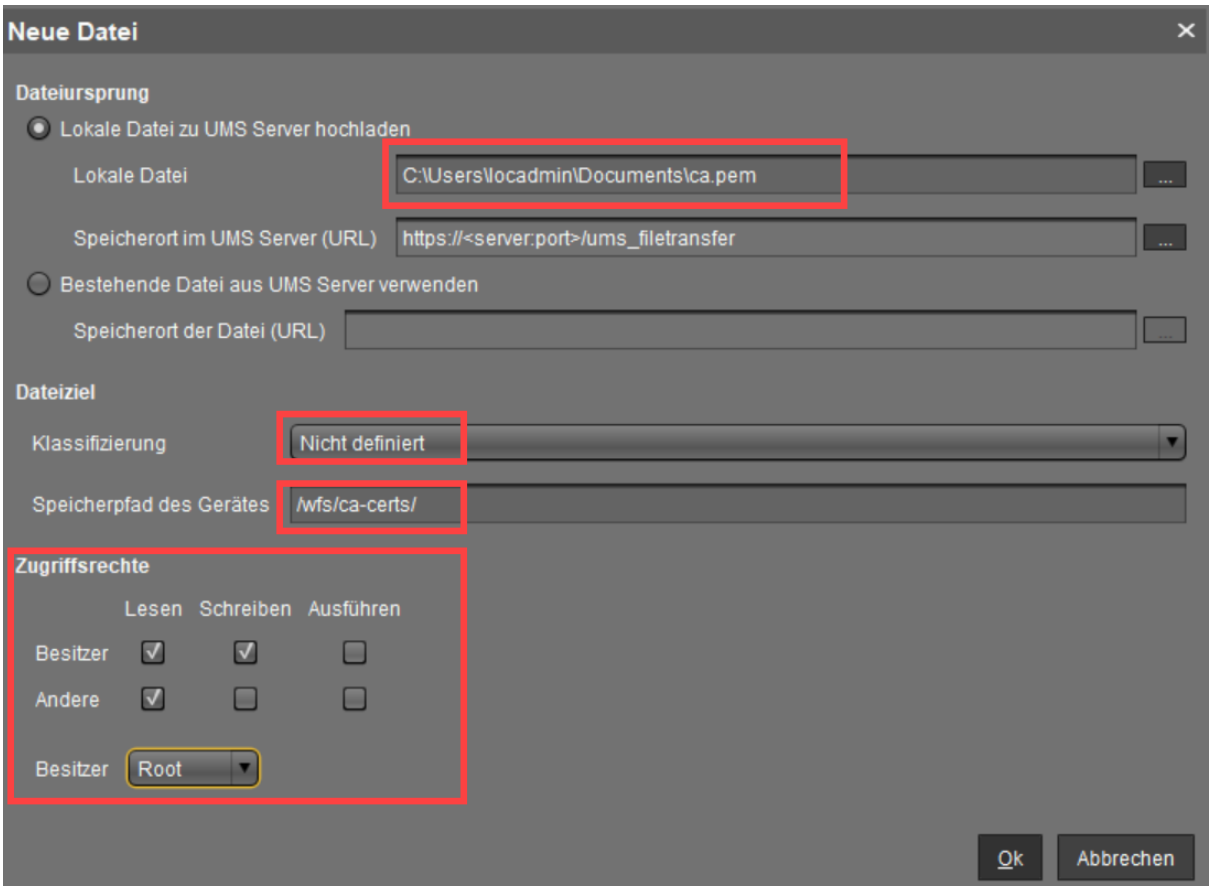
Installation des Zertifikats

Falls das X.509-Zertifikat Ihres Log-Collectors nicht von einer CA signiert ist, die IGEL OS bekannt ist, installieren Sie das CA-Root-Zertifikat des Unterzeichners wie folgt.

1. Legen Sie in der UMS Konsole unter **Dateien** per Rechtsklick eine **Neue Datei**.



2. Wählen Sie unter **Lokale Datei** die CA-Root-Zertifikatsdatei `ca.pem` im PEM-Format aus und laden Sie sie hoch.
3. Wählen Sie unter **Klassifizierung** "Nicht definiert".
4. Geben Sie bei **Speicherpfad des Gerätes** `/wfs/ca-certs/` ein.
5. Aktivieren Sie für den **Besitzer** Lese- und Schreibberechtigung, für **Andere** Leseberechtigung und setzen Sie den **Besitzer** auf **Root**.



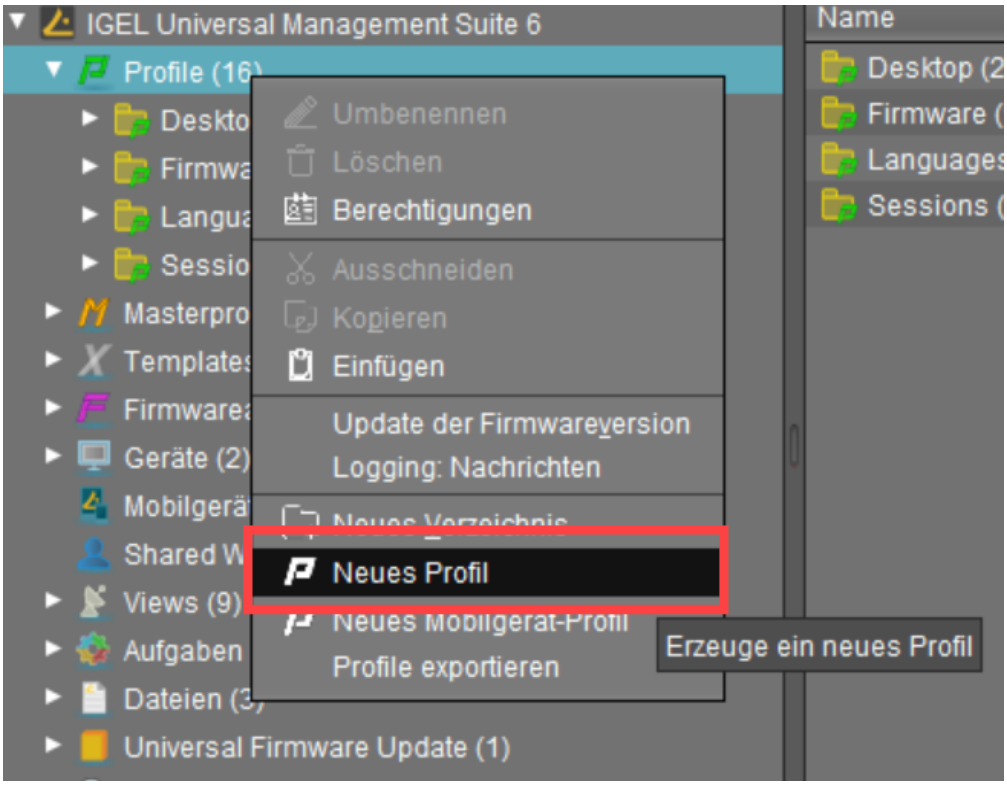
6. Klicken Sie **OK**.
7. Weisen Sie das Dateiobjekt den gewünschten Geräten zu.

Konfiguration der Protokollweiterleitung auf IGEL OS

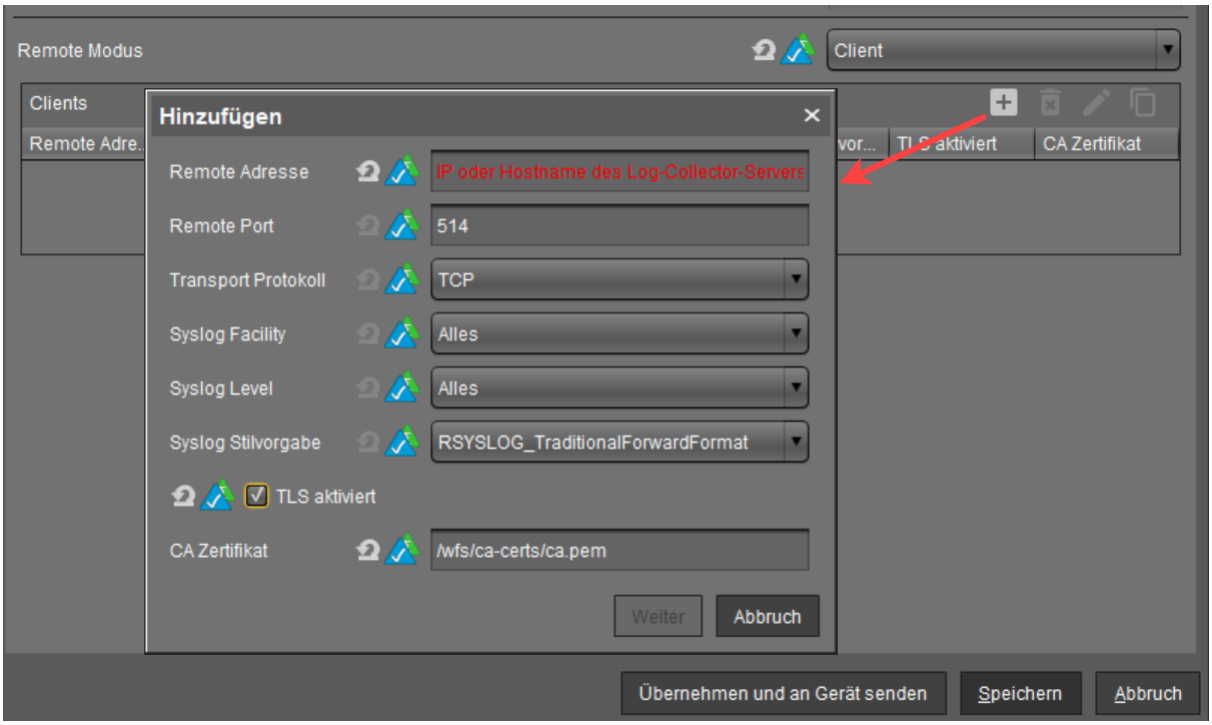
Ab IGEL OS 11.06.100 können Sie die Protokollweiterleitung mit TLS-Verschlüsselung wie folgt konfigurieren:

1. Erstellen Sie in der UMS ein neues Profil. Siehe Creating Profiles in the IGEL UMS[56].

56. https://kb.igel.com/en/universal-management-suite/current/creating-profiles-in-the-igel-ums



2. Gehen Sie im Konfigurationsdialog zu **System > Protokollierung**.
3. Setzen Sie **Remote Modus** auf "Client".
4. Klicken Sie die Schaltfläche **Hinzufügen**.
5. Nehmen Sie die erforderlichen Einstellungen vor und aktivieren Sie **TLS aktiviert**.
6. Geben Sie unter **CA-Zertifikat** den Pfad zum CA-Root-Zertifikat an, das Sie zuvor installiert haben, z. B. `/wfs/ca-certs/ca.pem`.



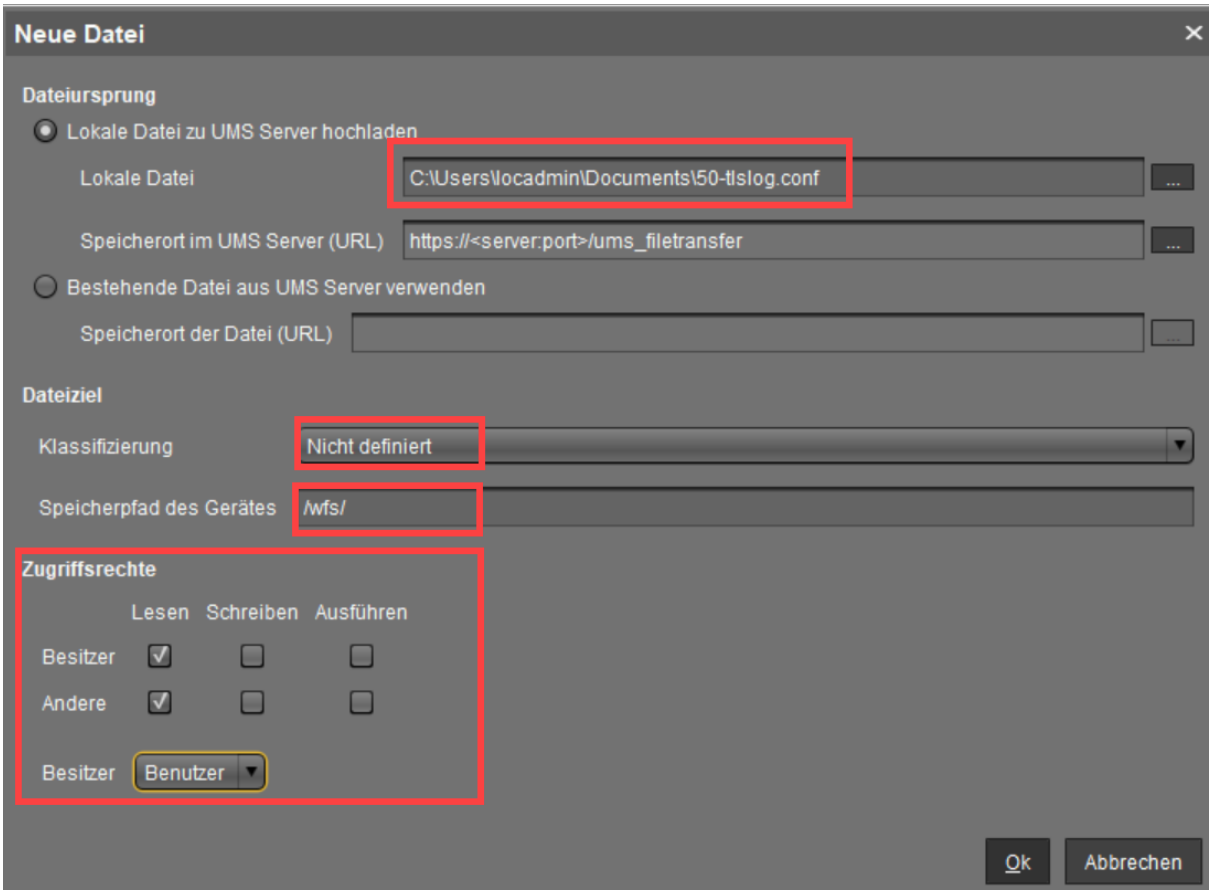
7. Speichern Sie die Änderungen und weisen Sie das Profil den gewünschten Geräten zu.
8. Starten Sie die Geräte neu, damit die Änderung wirksam wird.

Anweisungen für IGEL OS vor 11.06.100

In IGEL OS vor Version 11.06.100 konfigurieren Sie die Protokollweiterleitung mit TLS-Verschlüsselung wie folgt:

1. Erstellen Sie eine Textdatei `50-tlslog.conf` mit dem folgenden Inhalt:
   ```
   global(DefaultNetstreamDriverCAFile="/wfs/ca-certs/ca.pem")
   *.* action(type="omfwd" protocol="tcp"
   Target="<IP-Adresse oder DNS-Name des Log-Collectors>" port="<Port des Log-Collectors)"
    StreamDriver="gtls" StreamDriverMode="1"
   StreamDriverAuthMode="anon"
   template="RSYSLOG_TraditionalFileFormat")
   ```
2. Legen Sie in der UMS Konsole unter **Dateien** per Rechtsklick eine **Neue Datei** an.
3. Wählen Sie unter **Lokale Datei** die Datei `50-tlslog.conf` aus und laden Sie sie hoch.
4. Wählen Sie unter **Klassifizierung** "Nicht definiert".
5. Geben Sie bei **Speicherpfad des Gerätes** `/wfs/` ein.

6. Aktivieren Sie für den **Besitzer** und für **Andere** Leseberechtigung und setzen Sie den **Besitzer** auf **Benutzer**.



7. Klicken Sie **OK**.
8. Weisen Sie das Dateiobjekt den gewünschten Geräten zu.
9. Erstellen Sie ein Profil mit folgendem Inhalt:
    a. Gehen Sie im Konfigurationsdialog zu **System > Firmwareanpassung > Eigene Befehle > Basis**.
    b. Fügen Sie im Feld **Initialisierung** folgende Zeile ein:
    ```
    cp /wfs/50-tlslog.conf /etc/rsyslog.d/
    ```
10. Weisen Sie das Profil den gewünschten Geräten zu.
11. Starten Sie die Geräte neu, um die Änderung wirksam werden zu lassen.

Maßnahme: Konfigurationsänderungen analysieren

Daneben lassen sich in der Universal Management Suite verschiedene Protokolleinträge zu administrativen Tätigkeiten durchsuchen:

- Wählen Sie **System > Logging > Nachrichten**, um zu sehen, wann Einstellungen und Befehle an welches Gerät geschickt wurden.

- Wählen Sie **System > Logging > Ereignisse**, um Änderungen an Objekten in der Universal Management Suite anzuzeigen.
- Wählen Sie **System > Logging > Fernzugriff**, um herauszufinden, wann welcher UMS Benutzer welches Gerät mittels **Secure Shadowing** gespiegelt hat.

Datensicherung

Anforderung

Telearbeitsrechner sollten über Funktionen zur Datensicherung verfügen.

Maßnahmen

Alle Einstellungen und Dateien auf dem Thinclient müssen per Universal Management Suite auf den Thinclient ausgerollt werden. Andere lokale Dateien dürfen nicht gespeichert werden. Somit lässt sich das Backup des Thinclients durch ein Backup der Daten in der Universal Management Suite erledigen:

1. Starten Sie als Administrator die Anwendung **IGEL Universal Management Suite Administrator.**
2. Gehen Sie zu **Datensicherungen**.
3. Klicken Sie **Erzeugen**.
4. Vergeben Sie einen Namen für die Backupdatei.
5. Wählen Sie **Alle auswählen** als Datensicherungseinstellung.
6. Klicken Sie **OK**.

Verschlüsselung

Anforderung

Telearbeitsrechner sollten über eine Verschlüsselungskomponente verfügen.

Maßnahme: TLS-Suites in IGEL OS konfigurieren

1. Gehen Sie im Setup zu **System > Registry**
2. Setzen Sie den Parameter **system.security.remote_management.tls_policy** („TLS Richtlinie“) auf den Wert **BSI**.
3. Klicken Sie **Übernehmen**.

Maßnahme: TLS-Suites in UMS konfigurieren

1. Starten sie die Anwendung **UMS Administrator** mit Administratorrechten.
2. Klicken Sie auf der Seite **Einstellungen** die Schaltfläche **Cipher konfigurieren**.
3. Benutzen Sie die Schaltfläche **Deaktivieren**, um alle Cipher außer den folgenden zu deaktivieren:
   TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
   TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
   TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
   TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
   TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
   TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
   TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
   TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
   TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
   TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
   TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
   TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
4. Klicken Sie **OK**.
5. Klicken Sie auf Nachfrage **Server jetzt neu starten**.
6. Klicken Sie **Übernehmen**.

Anmerkung: SSH Ciphers

Folgende Algorithmen sind für den SSH-Daemon konfiguriert:

Ciphers aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com[57], aes256-gcm@openssh.com[58], chacha20-poly1305@openssh.com[59]

57. mailto:aes128-gcm@openssh.com
58. mailto:aes256-gcm@openssh.com
59. mailto:chacha20-poly1305@openssh.com

KexAlgorithms curve25519-sha256@libssh.org[60], ecdh-sha2-nistp521, ecdh-sha2-nistp384, ecdh-sha2-nistp256, diffie-hellman-group-exchange-sha256

MACs hmac-sha2-512-etm@openssh.com[61], hmac-sha2-256-etm@openssh.com[62], umac-128-etm@openssh.com[63], hmac-sha2-512, hmac-sha2-256, umac-128@openssh.com[64]

Anmerkung: Verschlüsselung des Massenspeichers

Die schreibbaren Bereiche des Massenspeichers (/wfs, Custom Partitions, Firefox-Profil-Partition) sind per LUKS2 mit dem Cipher AES-XTS-plain64 verschlüsselt. Der verwendete Schlüssel ist 512 bit lang und pro Hardwareeinheit eindeutig.

60. mailto:curve25519-sha256@libssh.org
61. mailto:hmac-sha2-512-etm@openssh.com
62. mailto:hmac-sha2-256-etm@openssh.com
63. mailto:umac-128-etm@openssh.com
64. mailto:umac-128@openssh.com

Virenschutz

Anforderung

In Abhängigkeit des installierten Betriebssystems und anderer vorhandener Schutzmechanismen des Telearbeitsrechners muss geprüft werden, ob Viren-Schutzprogramme eingesetzt werden sollen. Ist dies der Fall, muss vor dem Einspielen von Daten von auswechselbaren Datenträgern, vor der Weitergabe von Datenträgern beziehungsweise beim Senden und Empfangen von Daten ein Virencheck durchgeführt werden.

Anmerkung

Bei IGEL OS handelt es sich um Linux, das in der Regel nicht von Viren befallen wird. Daneben werden die Systempartitionen mit Schreibschutz eingehängt und mittels kryptografischer Signaturen die Integrität gewährleistet, was die Persistenz von etwaiger Malware verhindert. Aus diesem Grund verzichtet IGEL auf ein Viren-Schutzprogramm auf IGEL OS.

Systempflege

Maßnahme: IGEL OS-Version mit Maintenance einsetzen

Es muss eine IGEL OS-Version eingesetzt werden, die von IGEL mit Sicherheitsupdates versorgt wird.

- Erwerben Sie (kostenpflichtige) Maintenance von IGEL, um allen Sicherheitsupdates installieren zu dürfen.
- IGEL OS 11.x wird derzeit mit Sicherheitsupdates versorgt. Sollte IGEL die OS-Generation 11 abkündigen, erfolgt noch weitere 3 Jahre die Versorgung mit Sicherheitsupdates.

Maßnahme: Über Sicherheitsupdates informieren

- Die Verantwortlichen müssen sich über bekannt gewordene Schwachstellen informieren. Überprüfen Sie wöchentlich, ob es unter IGEL Product Security Information (see page 3) Sicherheitshinweise für IGEL OS 11 gibt und welche Maßnahme zu ergreifen sind, etwa Einspielen von Sicherheitsupdates.

Maßnahme: Referenzinstallation testen

- Sie sollten einen Thinclient für die Referenzinstallation von IGEL OS bereithalten. Ist ein eine IGEL OS-Version mit Sicherheitsupdates verfügbar, testen Sie auf diesem Gerät die erfolgreiche Behebung der Sicherheitsprobleme und stellen Sie sicher, dass die für den Betrieb benötigt Funktionalität noch immer bereitsteht.
- Richten Sie nach erfolgreichem Test auf der Referenzinstallation das IGEL OS-Update für die produktiven Thinclients ein.

Maßnahme: IGEL OS-Update einrichten

Es müssen jene Updates für IGEL OS eingespielt werden, die von IGEL vermeldete Sicherheitsprobleme beheben.

Beziehen Sie IGEL OS-Updates:

1. Suchen Sie in der UMS Console mit einem Rechtsklick auf **Universal Firmware Updates** nach Updates für Ihre Thinclients.
2. Aktivieren Sie die Checkbox für die Updates von **IGEL OS 11**.
3. Klicken Sie **Herunterladen**.

Ordnen sie das IGEL OS-Update dem Thinclient zu:

1. Ziehen Sie das gewünschte Universal Firmware Update im Navigationsbaum der UMS Console auf den Thinclient.
2. Wählen Sie im Dialog **Änderungszeitpunkt** die Option **Sofort** und klicken Sie **OK**.

Maßnahme: Automatisches IGEL OS-Update konfigurieren

Der Thinclient muss so konfiguriert sein, dass er automatisch täglich nach Updates sucht und diese installiert. Die folgenden Anweisungen stellen sicher, dass dies bei allen Thinclients täglich passiert, egal ob sie ausgeschaltet oder im Betrieb sind.

Automatische Updatesuche konfigurieren:

1. Gehen Sie im Setup zu **System > Update > Firmwareupdate.**
2. Aktivieren Sie die Checkbox **Automatische Updatesuche beim Herunterfahren**.
3. Klicken Sie **Übernehmen**.

Automatisches Wakeup und Update konfigurieren:

1. Gehen Sie in UMS Console im Navigationsbaum zu **Aufgaben**.
2. Rechtsklicken Sie **Aufgaben** und wählen Sie **Neue Aufgabe**.
3. Geben Sie der Aufgabe den Namen **Thinclients aufwecken**.
4. Wählen Sie **Wakeup** als **Befehl**.
5. Wählen Sie eine **Ausführungszeit**, zu der die Thinclients nicht in Benutzung sind.
6. Klicken Sie **Weiter**.
7. Konfigurieren Sie bei Aufgabe Wiederholen **Jeden 1 Tag**.
8. Klicken Sie **Weiter**.
9. Markieren Sie den Ordner **Geräte** unter zuweisbare Objekte und klicken Sie den Pfeil nach rechts (>), um die Geräte der Menge **Selektierte Objekte** hinzuzufügen.
10. Klicken Sie **Fertig**.
11. Rechtsklicken Sie **Aufgaben** und wählen Sie **Neue Aufgabe**.
12. Geben Sie der Aufgabe den Namen **Thinclients herunterfahren**.
13. Wählen Sie **Herunterfahren** als **Befehl**.
14. Wählen Sie eine **Ausführungszeit** 20 Minuten nach dem der Ausführungszeit der Aufgabe **Thinclients aufwecken**.
15. Klicken Sie **Weiter**.
16. Konfigurieren Sie bei Aufgabe Wiederholen **Jeden 1 Tag**.
17. Klicken Sie **Weiter**.
18. Markieren Sie den Ordner **Geräte** unter zuweisbare Objekte und klicken Sie den Pfeil nach rechts (>), um die Geräte der Menge **Selektierte Objekte** hinzuzufügen.
19. Klicken Sie **Fertig**.

Zusätzliche Anforderungen aus SYS.2

Anforderung: Wechsellaufwerke als nicht ausführbar einbinden

Maßnahme: Nicht-Ausführbar setzen

1. Gehen Sie im Setup zu **System > Registry**
2. Aktivieren Sie beim Parameter **autofs.noexec_option** die Option **Nicht-Ausführbar setzen**.
3. Klicken Sie **Übernehmen**.

Logging and Log Evaluation

Prerequisites

Teleworking computers should have a logging function and should have a log evaluation function.

Note

IGEL recommends leaving logging enabled by default (authentication, kernel, and daemons) and limiting the desired parameters by filtering during evaluation.

Action: Forward Logs to Log Analyzer

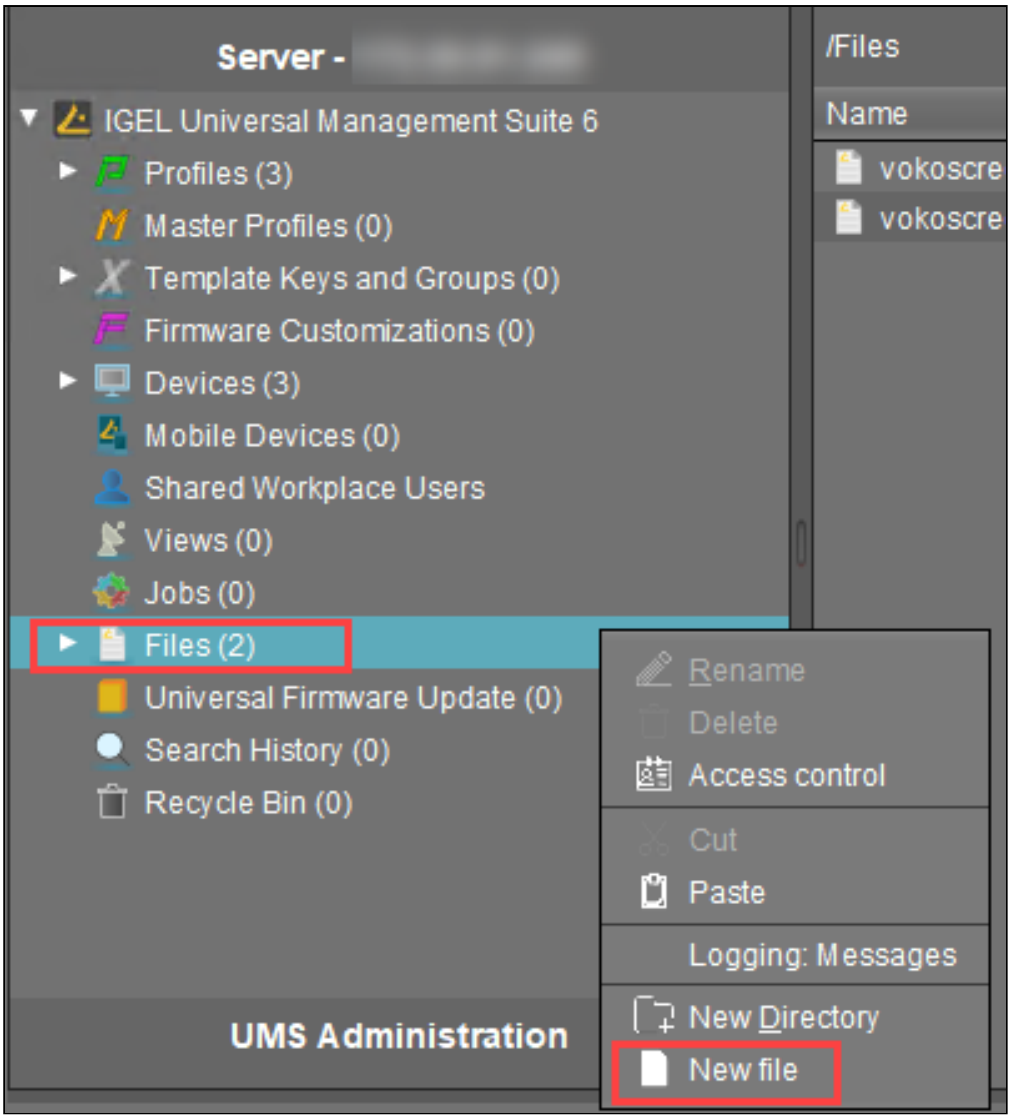
Use a log collector and analyzer, which allows the archiving and analysis of logs according to many aspects, such as Graylog, Splunk or the Elastic-Logstash-Kibana-Stack (ELK). Their evaluation function must be able to differentiate according to the types of data required for logging (for example, filtering all unauthorized access to all resources in a given period of time). The evaluation function must generate evaluable (readable) reports so that no security-critical activities are overlooked.

Such solutions can receive log data via rsyslog interface with TLS encryption. In IGEL OS, configure the forwarding as follows:

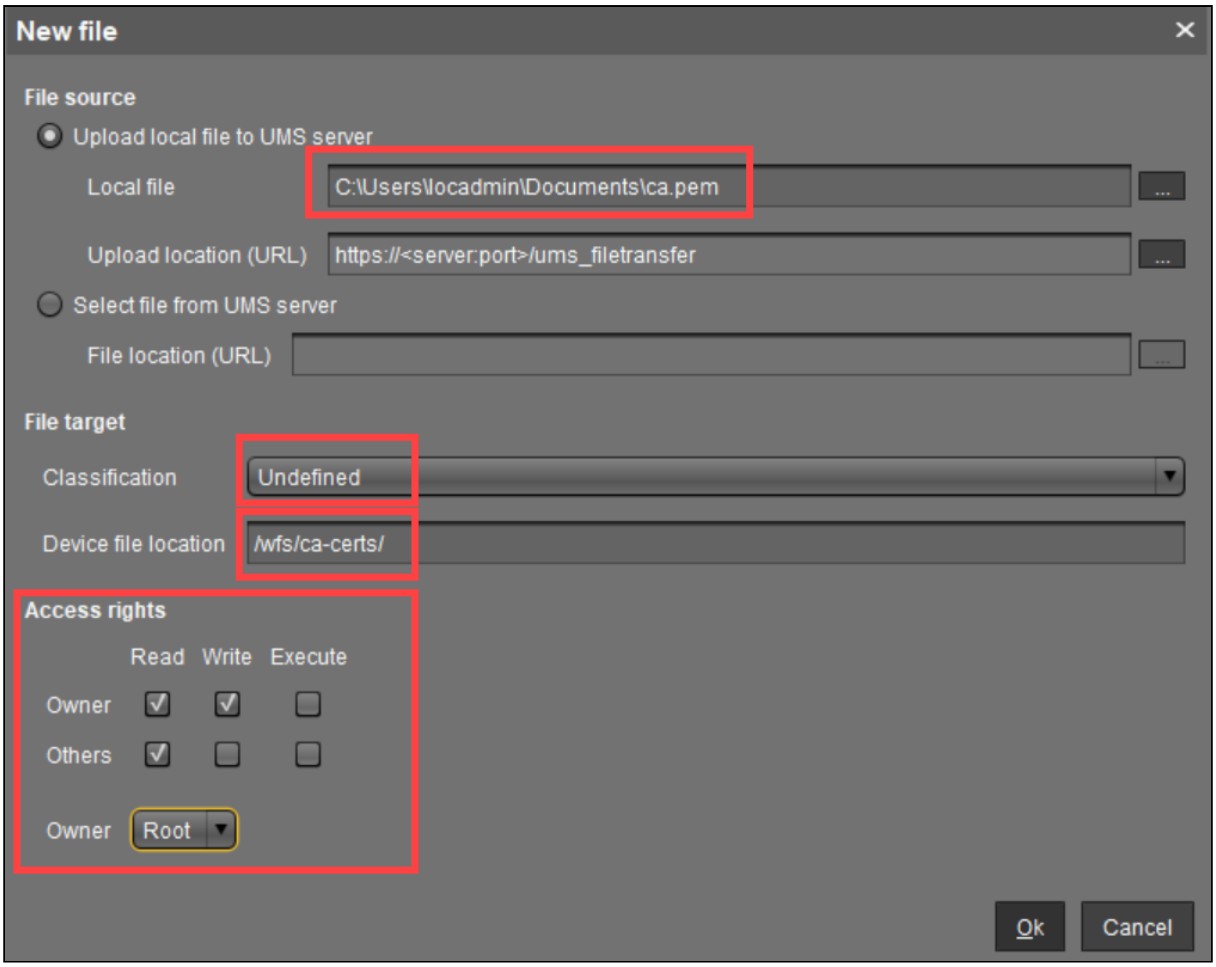
Installing the Certificate

If the X.509 certificate of your log collector is not signed by a CA known to IGEL OS, install the CA root certificate of the signer as follows:

1. Create a **new file** in the UMS Console under **Files** by right-clicking.



2. Under **Local file**, select the CA root certificate file `ca.pem` in PEM format and upload it.
3. Under **Classification**, select "Undefined".
4. Enter `/wfs/ca-certs/` for the **Device file location**.
5. Enable read and write permission for the **Owner**, read permission for **Others** and set the **Owner** to **Root**.

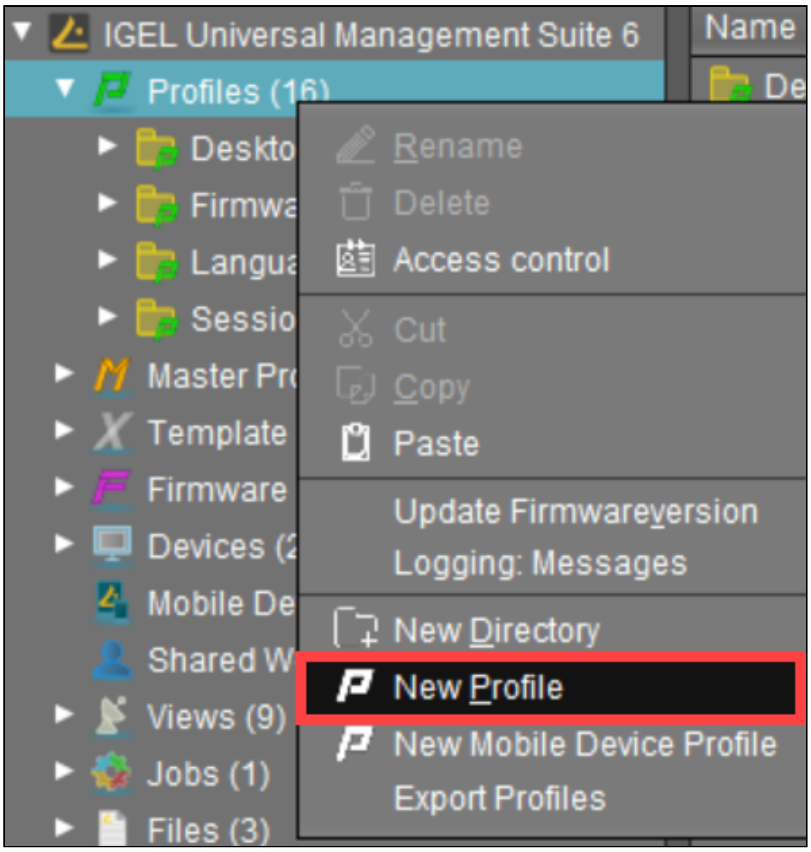


6. Click **Ok**.
7. Assign the file object to the desired devices.

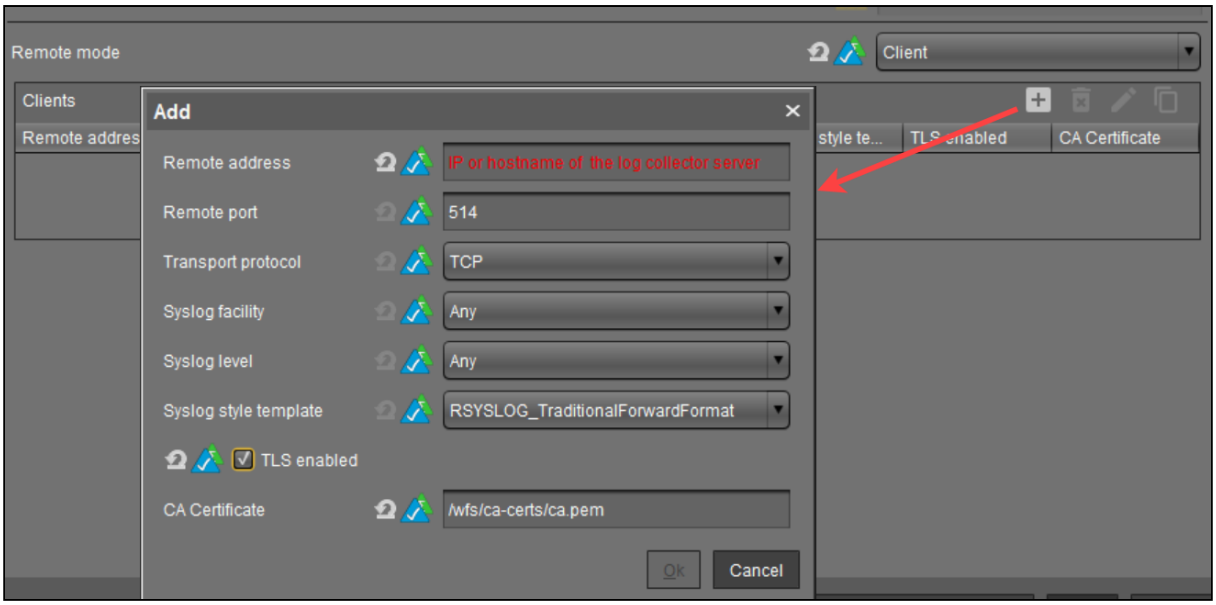
Configuration of Log Forwarding on IGEL OS

As of IGEL OS 11.06.100, you can configure the log forwarding with TLS encryption as follows:

1. In the UMS, create a new profile. See (12.05.100-en) Creating Profiles in the IGEL UMS .



2. In the configuration dialog, go to **System > Logging**.
3. Set **Remote mode** to "Client".
4. Click the **Add** button.
5. Make the required settings and activate **TLS enabled**.
6. Under **CA certificate**, specify the path to the CA root certificate you have installed previously, e.g. `/wfs/ca-certs/ca.pem`.

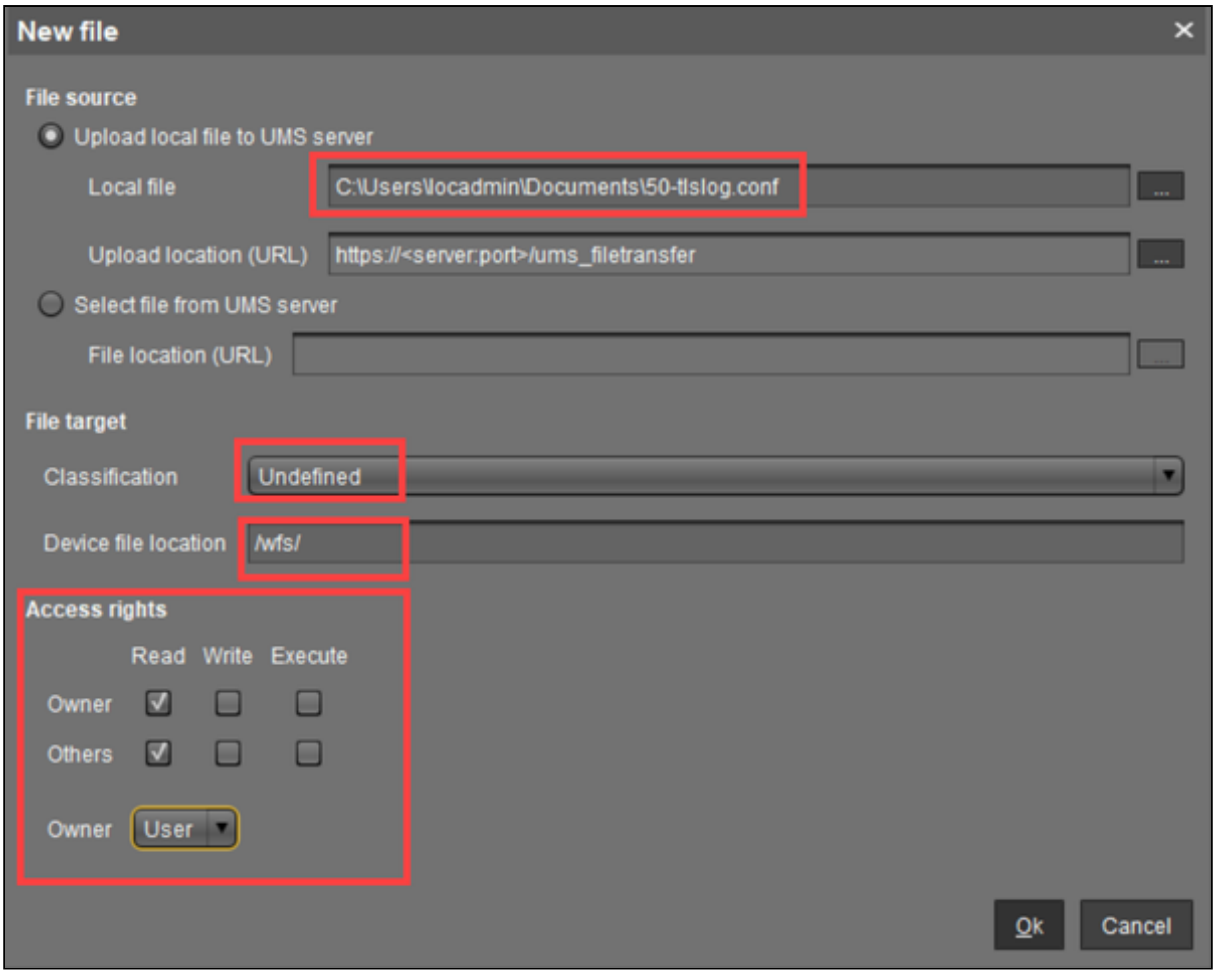


7. Save the changes and assign the profile to the desired devices.
8. Reboot the devices to make the change effective.

Instructions for IGEL OS before 11.06.100

In IGEL OS before version 11.06.100, configure the log forwarding with TLS encryption as follows:

1. Create a text file `50-tlslog.conf` with the following content:
   ```
   global(DefaultNetstreamDriverCAFile="/wfs/ca-certs/ca.pem")
   *.* action(type="omfwd" protocol="tcp"
   Target="<IP address or DNS name of the log collector>" port="<Port of the log collector)"
   StreamDriver="gtls" StreamDriverMode="1"
   StreamDriverAuthMode="anon"
   template="RSYSLOG_TraditionalFileFormat")
   ```
2. Create a **new file** in the UMS Console under **Files** by right-clicking.
3. Under **Local file**, select the file `50-tlslog.conf` and upload it.
4. Under **Classification**, select "Undefined".
5. Enter `/wfs/` under **Device file location**.
6. Enable read permission for the **Owner** and for **Others** and set the **Owner** to **User**.



7. Click **Ok**.
8. Assign the file object to the desired devices.
9. Create a profile with the following content:
    a. In the configuration dialog, go to **System > Firmware Customization > Custom Commands > Basic**.
    b. Enter the following line in the **Initialization** field:
    `cp /wfs/50-tlslog.conf /etc/rsyslog.d/`
10. Assign the profile to the desired devices.
11. Reboot the devices to make the change effective.

Action: Analyze Configuration Changes

In addition, various log entries for administrative activities can be searched in the Universal Management Suite:

- Choose **System > Logging > Log Messages** to see when settings and commands were sent to which device.
- Choose **System > Logging > Event Messages** to see changes to objects in the Universal Management Suite.

- Choose **System > Logging > Remote Access** to find out when which UMS user has shadowed which device using **Secure Shadowing**.

Anleitung zum IT-Grundschutz-konformen Betrieb von IGEL OS 12

This documentation is available in German only.

Über das Dokument

Dieses Dokument beschreibt, welche Einstellungen an einer IGEL OS 12 (und UMS 12)-Installation IGEL empfiehlt, um die Sicherheitsanforderungen aus dem IT-Grundschutz zu erfüllen. Es nennt nur jene Grundschutz-Bausteine und Anforderungen, zu denen IGEL-spezifische Hilfestellungen gegeben werden können.

Es beruht auf dem IT-Grundschutz-Kompendium, Stand Februar 2023.

OPS.1.1.2 Ordnungsgemäße IT-Administration

Standard-Anforderungen von OPS.1.1.2

OPS.1.1.2.A16 Erweiterte Sicherheitsmaßnahmen für Administrationszugänge (S)

Beschränken Sie den Zugriff auf UMS Console und UMS Web App auf einen einzelnen Host, an dem sich Administratoren authentisieren müssen, und dazu die MFA-Möglichkeiten des Host-Betriebssystems oder Identity Providers nutzen.

OPS.1.1.2.A23 Rollen- und Berechtigungskonzept für administrative Zugriffe (S)

- Verwenden Sie ausschließlich UMS 12 zur Administration.
- Schützen Sie das lokale Setup auf den OS-12-Geräten mit Root-Password.
- Entfernen Sie die Starter für das lokale Setup via UMS unter **Zubehör > Setup**.

Arbeiten Sie in UMS nicht als UMS-Superuser, sondern legen Sie in der UMS Console unter **System > Administratorkonten** Benutzerkonten für Administratoren an, siehe https://kb.igel.com/en/universal-management-suite/12.06.120/how-to-create-administrator-accounts-in-the-igel-u oder importieren Sie Administratorkonten aus Active Directory, siehe https://kb.igel.com/en/universal-management-suite/12.06.120/importing-active-directory-users.

- Vergeben Sie granulare Berechtigungen für Administratorkonten an Ordnern, Geräten und Aktionen vergeben, siehe https://kb.igel.com/en/universal-management-suite/12.06.120/access-rights.

OPS.1.1.2.A26 Backup der Konfiguration (S)

- Das Backup der Endgeräte-Konfigurationen findet vollständig durch ein Backup der UMS-Datenbank statt:
  - Entweder durch die Backup-Funktion des UMS Administrator, siehe https://kb.igel.com/en/universal-management-suite/12.06.120/creating-a-backup-of-the-igel-ums.
  - Oder durch Backup-Mechanismen des eingesetzten DBMS.

OPS.1.1.2.A27 Ersatz für zentrale IT-Administrationswerkzeuge (S)

Erhöhen Sie die Verfügbarkeit der UMS durch den Einsatz mehrerer Instanzen, synchronisiert:

- Entweder durch UMS High Availability (HA), siehe https://kb.igel.com/en/universal-management-suite/12.06.120/igel-ums-high-availability-ha.
- Oder durch Distributed UMS, siehe https://kb.igel.com/en/universal-management-suite/12.06.120/installing-the-distributed-igel-ums.

OPS.1.1.2.A28 Protokollierung administrativer Tätigkeiten (S)

- Aktivieren Sie UMS Remote Security Logging, siehe https://kb.igel.com/en/universal-management-suite/12.06.120/remote-security-logging-in-igel sowie das Logging in der UMS Web App, siehe https://kb.igel.com/en/universal-management-suite/12.06.120/logging-in-the-igel-ums-web-app.
- Leiten Sie die lokalen Logfiles mit geeigneter Software an einen Log Collector oder ein SIEM weiter.

Anforderungen bei erhöhtem Schutzbedarf von OPS.1.1.2

OPS.1.1.2.A18 Durchgängige Protokollierung administrativer Tätigkeiten (H)

- Siehe OPS.1.1.2.A28 (see page 330).

OPS.1.1.2.A19 Nutzung hochverfügbarer IT-Administrationswerkzeuge (H)

- Siehe OPS.1.1.2.A27 (see page 330).

OPS.1.1.2.A29 Monitoring der IT-Administrationswerkzeuge (H)

Überwachen Sie die Verfügbarkeit von UMS-Datenbank, UMS-Hostbetriebsystem und UMS-Netzwerkdiensten mit geeigneten Werkzeugen.

OPS.1.1.2.A30 Sicherheitsmonitoring administrativer Tätigkeiten (H)

- Überwachen Sie UMS-Hostbetriebsystem und UMS-Datenbank mit SIEM und IDS, siehe OPS.1.1.2.A28 (see page 330).
- Binden Sie UMS Remote Security Logging ins SIEM ein.

Basis-Anforderungen von OPS.1.1.2

OPS.1.1.2.A6 Schutz administrativer Tätigkeiten (B)

Verwenden Sie zur Administration ausschließlich UMS 12, nie das lokale Setup der OS 12-Endgeräte.

UMS 12 kann Benutzer gegen lokale Konten oder gegen Active Directory authentisieren. Eine weitere Option, den Zugriff auf UMS 12 zu kontrollieren, besteht darin, den Zugriff auf UMS Console und UMS Web App auf einen einzelnen Host zu beschränken, auf dem sich Administratoren authentisieren müssen.

UMS 12 und OS 12 verwenden TLSv1.3 zur Tansportverschlüsselung des Management-Protokolls.

OPS.1.1.3 Patch- und Änderungsmanagement

Basis-Anforderungen von OPS.1.1.3

OPS.1.1.3.A3 Konfiguration von Autoupdate-Mechanismen (B)

- Updates für OS 12 Basis-System und Apps können auf verschiedene Weise ausgelöst werden:
  - Auto-Update, sobald neue Versionen im Repository verfügbar sind, siehe https://kb.igel.com/en/igel-os-base-system/12.5/how-to-keep-your-igel-os-12-system-up-to-date#id-(12.5-en)HowtoKeepYourIGELOS12SystemuptoDate-SettingtheUMStoUpdateRegularlySettingtheUMStoUpdateRegularly.
  - Update durch Zuweisen einer neuen Version von OS 12 oder App in der UMS, siehe https://kb.igel.com/en/igel-os-base-system/12.5/how-to-keep-your-igel-os-12-system-up-to-date#id-(12.5-en)HowtoKeepYourIGELOS12SystemuptoDate-RollingouttheAppUpdateonAllDevicesRollingouttheAppUpdateonAllDevices.

Update-Einstellungen für OS 12 und seine Apps sind lokal durch Dateiberechtigungen von OS 12 geschützt sowie im Netzwerk durch die Transportverschlüsselung des Managementprotokolls (TLSv1.3).

⚠ Prüfen Sie alle neuen Versionen von OS 12 und Apps zunächst in einer Testumgebung, bevor Sie sie in der Produktivumgebung ausrollen.

OPS.1.1.3.A15 Regelmäßige Aktualisierung von IT-Systemen und Software (B)

Für OS 12 und seine Apps sowie für UMS 12 veröffentlichen IGEL und seine Partner regelmäßig Aktualisierungen mit Sicherheitspatches.

- Informieren Sie sich in den IGEL Security Notices (ISN) über wichtige und kritische Sicherheitsaktualisierungen unter https://kb.igel.com/security-safety/current/igel-product-security-information.
- Lesen Sie die Release Notes zu den Aktualisierungen unter https://kb.igel.com/release-notes/current/.
- Verwenden sie IGEL OS 12 und UMS 12 nur während deren Wartungszeitraum – derzeit hat IGEL noch keine Termine für End-of-Life (EOL) und End-of-Maintenance (EOM) gesetzt.

Standard-Anforderungen von OPS.1.1.3

OPS.1.1.3.A8 Sicherer Einsatz von Werkzeugen für das Patch- und Änderungsmanagement (S)

- Verwenden Sie UMS 12 für das Patchmanagement für OS 12 und seine Apps.
- Sichern Sie UMS 12 ab, siehe OPS.1.1.2.A6 und OPS.1.1.2.A16

OPS.1.1.3.A10 Sicherstellung der Integrität und Authentizität von Softwarepaketen (S)

- Prüfen Sie vor der Erstinstallation IGEL OS 12 und UMS die heruntergeladenen Dateien gegen die auf http://igel.com angegeben Hashwerte.
- IGEL OS 12-Aktualisierungen sowie Apps sind mit Hashes und digitalen Signaturen versehen, die der in OS 12 eingebaute Update-Prozess vor dem Einspielen automatisch verifiziert.
- Verwenden Sie nur Apps, die von IGEL und seinen IGEL-Ready-Partnern zur Verfügung gestellt werden.
- Verwenden Sie ggf. Apps, die Sie in Ihrer Organisation selbst paketiert haben.

Anforderungen bei erhöhtem Schutzbedarf von OPS.1.1.3

OPS.1.1.3.A12 Einsatz von Werkzeugen beim Änderungsmanagement (H)

- Verwenden Sie UMS 12, da es Konfigurationen für OS 12 sicher und nachvollziehbar ausrollen kann.
- UMS 12 kann Konfigurationsänderungen auch wieder zurücknehmen.

OPS.1.1.3.A14 Synchronisierung innerhalb des Änderungsmanagements (H)

- Verwenden Sie UMS 12. OS 12 fragt die jüngsten Konfigurationen, Updates und Kommandos beim Systemstart ab, und auch wenn die Netzwerkverbindung zu UMS 12 nach einer Störung wieder verfügbar ist.

OPS.1.1.4 Schutz vor Schadprogrammen

Basis-Anforderungen von OPS.1.1.4

OPS.1.1.4.A2 Nutzung systemspezifischer Schutzmechanismen (B)

UMS 12 kann mit handelsüblichen Anti-Malware Lösungen auf dem Hostsystem betrieben werden.

OS 12 bietet die folgenden Schutzmechanismen vor Schadsoftware:

- Die Systempartition wird im Read-only-Modus betrieben: Malware kann keine Persistenz erlangen.
- Die Integrität der Systempartitionen wird durch Hashes und Signaturen gewährleistet, die überprüft werden:
    - Beim Systemstart
    - Zur Laufzeit
    - Vor der Anwendung von Aktualisierungen.

Sollte die Verifikation einer Signatur fehlschlagen, wird der Anwender sichtbar gewarnt.

- Die Trennung der Berechtigungen zwischen Administrator und Benutzer wirkt der Installation und Ausbreitung von Schadsoftware entgegen.

OPS.1.1.5 Protokollierung

- Basis-Anforderungen von OPS.1.1.5 (see page 340)

Basis-Anforderungen von OPS.1.1.5

OPS.1.1.5.A3 Konfiguration der Protokollierung auf System- und Netzebene (B)

UMS 12:

- Aktivieren Sie die Protokollierung der Benutzeraktionen in der UMS Konsole, siehe https://kb.igel.com/endpointmgmt-12.04.120/de/benutzeraktionen-protokollieren-126852245.html.
- Aktivieren Sie die Aufzeichnung sicherheitsrelevanter Ereignisse in UMS, siehe https://kb.igel.com/endpointmgmt-12.04.120/de/logging-126852118.html#Logging-SicherheitsrelevanteEreignisseaufzeichnen Die Ereignisse werden in Dateien protokolliert, die von einem konfigurierten Log Collector (z.B. Graylog) abgeholt werden können.

OS 12:

- Die lokalen Systemprotokolle lassen sich über die Rsyslog-Schnittstelle (TLS-verschlüsselt) an einen Log Collector oder ein SIEM weiterleiten, siehe https://kb.igel.com/base_system/12.4/en/logging-122896199.html#Logging-RemoteModeSwitchedtoClient.

OPS.1.1.5.A4 Zeitsynchronisation der IT-Systeme (B)

- **OS 12:** Konfigurieren Sie einen oder mehrere NTP-Server Ihrer Wahl, siehe https://kb.igel.com/base_system/12.4/en/time-and-date-122896178.html.
- **UMS 12:** Konfigurieren Sie einen NTP-Server Ihrer Wahl im Host-Betriebssystem der UMS.

OPS.1.2.5 Fernwartung

OPS.1.2.5.A2 Sicherer Verbindungsaufbau bei der Fernwartung von Clients (B) [Benutzende]

- Vor dem Spiegeln seines Desktops wird der Benutzer per Dialog gefragt, ob er das Spiegeln zulassen möchte. Während des Spiegelns wird ein visueller Hinweis angezeigt.
- Vor der Anwendung von Änderungen und vor einem System Neustart wird der Benutzer um Erlaubnis gefragt.

OPS.1.2.5.A3 Absicherung der Schnittstellen zur Fernwartung (B)

- Die Fernwartung von OS 12 ist nur von jener UMS-12-Installation möglich, an der das Betriebssystem registriert wurde. Dies wird durch Zertifikate sichergestellt.
- Die Fernwartungsverbindung ist transportverschlüsselt mit TLSv1.3

Standard-Anforderungen von OPS.1.2.5

OPS.1.2.5.A8 Sichere Protokolle bei der Fernwartung (S)

- Die Fernwartungsverbindung ist transportverschlüsselt mit TLSv1.3

OPS.1.2.5.A9 Auswahl und Beschaffung geeigneter Fernwartungswerkzeuge (S)

- Ist durch den Einsatz von UMS 12 gegeben.

Anforderungen bei erhöhtem Schutzbedarf von OPS1.2.5

OPS.1.2.5.A14 Dedizierte Clients und Konten bei der Fernwartung (H)

- Ist durch den Einsatz von UMS 12 gegeben.

SYS.2.1 Allgemeiner Client

Basis-Anforderungen von SYS.2.1

SYS.2.1.A1 Sichere Authentisierung von Benutzenden (B)

- Konfigurieren Sie ein Root-Passwort für das OS-12-Gerät.
- Setzen Sie Authentisierung für Benutzende ein (via UMS-Profil):
    - Ein lokales Benutzerkonto
    - ODER Authentisierung gegen on-premise Active Directory (AD) mit Kerberos
    - ODER Single Sign-On gegen einen Identitätsanbieter wie
        - Microsoft Entra ID
        - Okta
        - Open ID Connect
        - Ping Identity | Ping One
        - VMware Workspace One Access
    - ODER Authentisierung mit Smartcard
- Weitere Authentisierungslösung wie Imprivata, Evidian, etc. sind von OS 12 unterstützt.
- Verwenden Sie NICHT die Anmeldung als Gast, da hier keine Authentisierung stattfindet.
- Verwenden Sie automatische Bildschirmsperre
  o Stellen Sie die Bildschirmsperre so ein, dass nach einigen Minuten Inaktivität des Benutzers automatisch der Bildschirm gesperrt wird.
  o Lassen Sie zum Entsperren das Benutzerpasswort abfragen.
  o Optional können Sie auch das Administratorpasswort zum Entsperren zulassen.

SYS.2.1.A3 Aktivieren von Autoupdate-Mechanismen (B)

Siehe OPS.1.1.3.A3 (see page 334)Konfiguration von Autoupdate-Mechanismen (B)

SYS.2.1.A6 Einsatz von Schutzprogrammen gegen Schadsoftware (B)

Siehe OPS.1.1.4 Schutz vor Schadprogrammen (see page 337).

SYS.2.1.A8 Absicherung des Bootvorgangs (B)

OS 12 verwendet UEFI Secure Boot sowie signierte System- und Software-Partitionen, um die Integrität des Bootvorgangs sowie des Systems zu schützen.

- Aktivieren Sie UEFI Secure Boot im UEFI/BIOS des Geräts – häufig ist es schon aktiviert.
- Bei als “Secured-Core-PCs“ vermarkteten Geräten kann es erforderlich sein, die Einstellung „"Allow Microsoft 3rd Party UEFI CA" zu aktivieren, siehe https://kb.igel.com/securitysafety/en/secured-core-pcs-microsoft-3rd-party-uefi-certificate-for-secure-boot-70156597.html. Mit dieser CA signiert Microsoft im Namen des UEFI Forum IGEL OS und andere 3rd-Party-Betriebssysteme.
- Deaktivieren Sie im UEFI/BIOS das Booten von Wechselmedien wie USB-Sticks.
- Setzen Sie ein UEFI/BIOS -Passwort, um die obigen Einstellungen vor unberechtigter Änderung zu schützen.
- Informationen zu den oben genannten Schritten finden Sie in der Dokumentation Ihres BIOS-Herstellers.

SYS.2.1.A42 Nutzung von Cloud- und Online-Funktionen (B) [Benutzende]

Eine typische OS-12-Installation verwendet die folgenden, notwendigen Cloud- und Online-Funktionen:

- Management durch UMS: Unverzichtbar bis auf sehr spezielle Ausnahmen, dann aber potenziell Konflikt mit OPS.1.1.2.
- Die unverzichtbaren Betriebssystem-Updates und Apps kann das Endgerät entweder vom direkt IGEL App Portal (Cloud) oder via IGEL UMS (on-premise) beziehen. Dokumentieren Sie Ihre Entscheidung.
- Optional: Management via IGEL Cloud Gateway (ICG)
- Produktive Sitzungen für den Betrieb des Kunden (Web Browser, Citrix, Cisco Webex, Azure Virtual Desktop, Windows 365, RDP, Horizon und weitere): Verwenden Sie ausschließlich die für Ihren Betrieb benötigten und dokumentierten Sitzungen.
- Hilfsdienste für Drucken, Monitoring, Logging, Zugriffskontrolle (CUPS, ControlUp, deviceTrust, Imprivata und weitere). Verwenden Sie ausschließlich die für Ihren Betrieb benötigten und dokumentierten Hilfsdienste.
- Der IGEL Insight Service ist nicht für den Betrieb erforderlich. Stellen Sie sicher, dass er in **UMS Web App > Network > Settings > UMS Features** deaktiviert ist.

Standard-Anforderungen von SYS.2.1

SYS.2.1.A11 Beschaffung von Clients (S)

IGEL versorgt eine Produktgeneration (z.B. IGEL OS 12, UMS 12) mindestens 3 Jahre mit Bug- und Security-Fixes sowie neuen Features. Bis 3 Jahre nach dem Verkaufsende einer Produktgeneration stellt IGEL noch Security-Fixes dafür zur Verfügung, siehe https://kb.igel.com/en/igel-subscription-and-more/current/igel-product-lifecycle.

Derzeit hat IGEL für OS 12 und UMS 12 noch keine Termine für End-of-Life (EOL) und End-of-Maintenance (EOM) gesetzt.

SYS.2.1.A13 Zugriff auf Ausführungsumgebungen mit unbeobachtbarer Codeausführung (S)

Schützen Sie BIOS- und UEFI-Einstellungen durch ein BIOS-Passwort. Falls Ihr BIOS/UEFI sich mit Tools unter OS 12 managen lässt, ist dies nur als Root-Benutzer möglich.

SYS.2.1.A15 Sichere Installation und Konfiguration von Clients (S)

- Prüfen Sie bei den Installationsmedien **OS Creator**, **Base System Image for PXE**, **Base System Deployment Tool for SCCM** und **Universal Management Suite (UMS)** die SHA-265-Hashwerte Ihrer heruntergeladenen Dateien gegen die auf der IGEL-Homepage angegeben Werte.
- Prüfen Sie, dass alle Endpunkte an der gewünschten, dokumentierten UMS-Instanz registriert sind. In **Starter für Sitzungen > Informationen** auf OS 12 können Sie die IP-Adresse der verbundenen UMS-Instanz sehen.
- Bevorzugen Sie bei Apps jene, die von IGEL selbst (siehe Feld „Author“) oder von einem **IGEL Ready Developer** hergestellt wurden. Daneben gibt es die Möglichkeit, selbst Apps mit dem IGEL App Creator Portal zu paketieren – achten Sie hier auf die Vertrauenswürdigkeit des Autors des Recipe. Schließlich können Sie auch Community Apps installieren – hier liegt die Bewertung des Autors ganz bei Ihnen.
- Verwenden Sie bei der Konfiguration der Endpunkte die Empfehlungen aus diesem Dokument.
- Alle Einstellungen sind in UMS-Profilen einsehbar und reproduzierbar.

SYS.2.1.A16 Deaktivierung und Deinstallation nicht benötigter Komponenten und Kennungen (S)

- Durch die Trennung von Basissystem und Apps in OS 12 sind nach einer Standardinstallation nur notwendige Komponenten installiert. Falls nicht benötigt, kann in einem UMS-Profil noch folgendes deaktiviert werden:
  - Deaktivieren Sie den Zugriff auf virtuelle Linux-Konsolen in **Benutzeroberfläche > Bildschirm-Einstellungen > Zugriffskontrolle > Konsolenzugriff abschalten**.
  - Wenn Sie keine Smartcards verwenden, deaktivieren sie den PC/SC-Dämon in **Sicherheit > Smartcard > Dienste > PC/SC-Dämon aktivieren**.
- Alle Einstellungen sind in UMS-Profilen einsehbar und reproduzierbar.
- In der Standardeinstellung sind nur benötigte Benutzerkonten vorhanden – der nichtprivilegierte Benutzer *user* und der Linux-Superuser *root*, daneben benötigte Konten für Systemdienste.

SYS.2.1.A18 Nutzung von verschlüsselten Kommunikationsverbindungen (S)

- Kommunikationsverbindungen zu UMS, ICG sowie zu IGEL-Cloud-Diensten sind mit TLSv1.3 transportverschlüsselt.

SYS.2.1.A20 Schutz der Administrationsverfahren bei Clients (S)

- Administration ist auf dem Endgerät nur dem Linux-Superuser *root* oder einem optional einzurichtenden *Setup-Administrator* möglich. Administration durch UMS ist nur dem *UMS-Superuser* oder dort eingerichteten Administratorkonten möglich.

SYS.2.1.A21 Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und Kameras (S)

- Kamera und Mikrofon werden nur von bestimmten Apps verwendet, deren Installation in den Händen der UMS-Administratoren liegt.
    - Bei Web Browsern wird der Benutzer zusätzlich noch vom Browser um Erlaubnis gefragt.

SYS.2.1.A23 Bevorzugung von Client-Server-Diensten (S)

- Die Administration von OS 12 durch UMS (auch via ICG) erfolgt in Client-Server-Architektur, ebenfalls der Bezug von Lizenzen vom IGEL License Portal und die Installation von Apps aus dem IGEL App Portal.

SYS.2.1.A24 Umgang mit externen Medien und Wechseldatenträgern (S)

- In der Standardeinstellung von OS 12 werden Wechselmedien nicht automatisch eingebunden.
- Unter **Geräte > USB-Zugriffskontrolle** lassen sich zudem USB-Geräte nach Klasse (etwa Eingabegerät oder Massenspeicher) sowie nach Hersteller-ID, Geräte-ID und UUID erlauben oder verbieten.

SYS.2.1.A26 Schutz vor Ausnutzung von Schwachstellen in Anwendungen (S)

- Kernel ASLR Address (Space Layout Randomization) ist aktiviert.

SYS.2.1.A27 Geregelte Außerbetriebnahme eines Clients (S)

- Architekturbedingt sind auf dem Gerät nur Konfigurationsdaten vorhanden, und die enthaltende Partition ist verschlüsselt.
- Das Zurücksetzen eines Geräts auf Werkseinstellungen (lokal oder via UMS) löscht die Konfigurationspartition sowie die Datenpartitionen der Apps.

SYS.2.1.A34 Kapselung von sicherheitskritischen Anwendungen und Betriebssystemkomponenten (S)

- OS 12 verwendet AppArmor zur Sicherung ausgewählter Systemkomponenten.

SYS.2.1.A43 Lokale Sicherheitsrichtlinien für Clients (S)

- Werden durch UMS-Profile und Empfehlungen dieses Dokuments umgesetzt.

Anforderungen bei erhöhtem Schutzbedarf von SYS.2.1

SYS.2.1.A28 Verschlüsselung der Clients (H)

- Aktivieren Sie die Geräteverschlüsselung unter **Sicherheit > Geräteverschlüsselung.**
- Verwenden Sie ein langes Passwort.
- Verwenden Sie TPM mit PIN und PCR, soweit von Ihrer Gerätehardware unterstützt.

SYS.2.1.A29 Systemüberwachung und Monitoring der Clients (H)

- Die lokalen Systemprotokolle lassen sich über die Rsyslog-Schnittstelle (TLS-verschlüsselt) an einen Log Collector oder ein SIEM weiterleiten, siehe https://kb.igel.com/base_system/12.4/en/logging-122896199.html#Logging-RemoteModeSwitchedtoClient.

SYS.2.1.A30 Einrichten einer Referenzumgebung für Clients (H)

- UMS-Profile mit erfolgreich getesteten Einstellungen lassen sich einfach aus einer Referenz-Umgebung in eine Produktivumgebung übertragen.

SYS.2.1.A31 Einrichtung lokaler Paketfilter (H)

- Iptables/nftables sind im Basissystem von OS 12 enthalten.
- Iptables/nftables-Skripte können in UMS-Profilen in **System > Systemanpassung > Eigene Befehle > Basis > Initialisierung** auf die Endgeräte ausgerollt werden.

SYS.2.1.A32 Einsatz zusätzlicher Maßnahmen zum Schutz vor Exploits (H)

OS 12 bietet die folgenden Schutzmechanismen vor Schadsoftware:

- Die Systempartition wird im Read-only-Modus betrieben: Malware kann keine Persistenz erlangen.
- Die Integrität der Systempartitionen wird durch Hashes und Signaturen gewährleistet, die überprüft werden:
    - Beim Systemstart
    - Zur Laufzeit
    - Vor der Anwendung von Aktualisierungen.

Sollte die Verifikation einer Signatur fehlschlagen, wird der Anwender sichtbar gewarnt.

- Die Trennung der Berechtigungen zwischen Administrator und Benutzer wirkt der Installation und Ausbreitung von Schadsoftware entgegen.

SYS.2.1.A33 Einsatz von Ausführungskontrolle (H)

- Nicht vorhanden in IGEL OS 12.

SYS.2.1.A35 Aktive Verwaltung der Wurzelzertifikate (H)

- Wurzelzertifikate für Secure Boot werden durch UEFI/BIOS-Hersteller und den Kunden verwaltet.

- In OS 12 im globalen Truststore /etc/ssl/certs vorinstallierte Wurzelzertifikate sind im README der OS-12-Release dokumentiert, wenn Sie aktualisiert wurden.
- Wurzelzertifikate für bestimmte Zwecke wie SCEP, IEEE 802.1X oder VPN lassen sich über UMS-Profile installieren.

SYS.2.1.A36 Selbstverwalteter Einsatz von SecureBoot und TPM (H)

- UEFI Shim ist von Microsoft signiert, Kernel und Partitionen von IGEL.
- TPM kann vom Kunden zum Absichern des Schlüssels für die Festplattenverschlüsselung verwendet werden.

SYS.2.1.A37 Verwendung von Mehr-Faktor-Authentisierung (H)

- OS 12 bietet zahlreiche MFA-Optionen für die lokale Anmeldung:
  - z.B. per Microsoft Entra ID mit Microsoft Authenticator App.
  - Durch die Unterstützung weiterer Identity Provider, die MFA-Optionen bieten.

SYS.2.1.A41 Verwendung von Quotas für lokale Datenträger (H)

- OS 12 verwendet keine Quotas für Dateisysteme.

SYS.2.1.A45 Erweiterte Protokollierung (H)

- Die lokalen Systemprotokolle lassen sich über die Rsyslog-Schnittstelle (TLS-verschlüsselt) an einen Log Collector oder ein SIEM weiterleiten, siehe https://kb.igel.com/base_system/12.4/en/logging-122896199.html#Logging-RemoteModeSwitchedtoClient

SYS.2.3 Clients unter Linux und Unix

Standard-Anforderungen von SYS.2.3

SYS.2.3.A6 Kein automatisches Einbinden von Wechsellaufwerken (S) [Benutzende]

- In der Standardeinstellung von OS 12 werden Wechselmedien nicht automatisch eingebunden.
- Wechsellaufwerke lassen sich als nicht-ausführbar einhängen:

1. Gehen Sie im Setup zu **System > Registry**
2. Aktivieren Sie beim Parameter **devices.autofs.noexec_option** die Option **Nicht-Ausführbar setzen**.
3. Klicken Sie **Übernehmen**.

SYS.2.3.A7 Restriktive Rechtevergabe auf Dateien und Verzeichnisse (S)

- IGEL OS verwendet restriktive Rechtevergabe: Betriebssystem und Applikationen können nicht vom nicht-privilegierten *user* verändert werden.
- Daneben wird das Betriebssystem als Read-only-Partition eingehängt.

SYS.2.3.A8 Einsatz von Techniken zur Rechtebeschränkung von Anwendungen (S)

IGEL OS 12 verwendet AppArmor, um die Berechtigungen des Dienstes dhcpcd im Basissystem einzuschränken. Für installierte Apps besteht derzeit keine Einschränkung dorch AppArmor.

Somit ist die Anforderung teilweise erfüllt.

Als mitigierenden Faktor bis zur vollständigen Erfüllung empfiehlt IGEL, nur folgende App-Kategorien aus dem IGEL App Portal zu installieren, da sie einen Security-Review durch IGEL erhalten:

- Von IGEL selbst paketierte Apps (Herausgeber: IGEL Technology GmbH)
- Von IGEL Ready Partnern paketierte Apps (Kategorie: IGEL Ready)

SYS.2.3.A9 Sichere Verwendung von Passwörtern auf der Kommandozeile (S) [Benutzende]

- In der Regel bekommen Benutzende keine Kommandozeile zur Befehlsausführung zur Verfügung gestellt.

SYS.2.3.A11 Verhinderung der Überlastung der lokalen Festplatte (S)

- IGEL OS 12 nutzt unterschiedliche Partitionen für System und Konfigurationsdaten. Speichern von Nutzdaten ist in der Architektur nicht vorgesehen.
- Es werden keine Quotas verwendet, allerdings ist die Systempartition Read-only eingehängt.

Anforderungen bei erhöhtem Schutzbedarf von SYS.2.3

SYS.2.3.A14 Absicherung gegen Nutzung unbefugter Peripheriegeräte (H)

- Unter **Geräte > USB-Zugriffskontrolle** lassen sich USB-Geräte nach Klasse (etwa Eingabegerät oder Massenspeicher) sowie nach Hersteller-ID, Geräte-ID und UUID erlauben oder verbieten.

SYS.2.3.A15 Zusätzlicher Schutz vor der Ausführung unerwünschter Dateien (H)

- Wechsellaufwerke lassen sich als nicht-ausführbar einhängen:

1. Gehen Sie im Setup zu **System > Registry**
2. Aktivieren Sie beim Parameter **devices.autofs.noexec_option** die Option **Nicht-Ausführbar setzen**.
3. Klicken Sie **Übernehmen**.

SYS.2.3.A17 Zusätzliche Verhinderung der Ausbreitung bei der Ausnutzung von Schwachstellen (H)

- OS 12 verwendet AppArmor zur Sicherung ausgewählter Systemkomponenten.

SYS.2.3.A18 Zusätzlicher Schutz des Kernels (H)

- OS 12 verwendet keine zusätzlichen Patches zur Härtung des Linux-Kernels.

SYS.2.3.A19 Festplatten- oder Dateiverschlüsselung (H)

- Die Festplattenpartition für die schreibbaren Daten (Konfiguration) ist mit AES-246 im XTS-Modus verschlüsselt, dabei wird dm-crypt genutzt.
- TPM, falls auf der Hardware verfügbar, kann vom Kunden zum Absichern des Schlüssels für die Festplattenverschlüsselung verwendet werden.

SYS.2.3.A20 Abschaltung kritischer SysRq-Funktionen (H)

- Kritische SysRq-Funktionen sind in OS 12 begrenzt.

Basis-Anforderungen von SYS.2.3

SYS.2.3.A1 Authentisierung von Administrierenden und Benutzenden (B) [Benutzende]

- Benutzer melden sich im Normalbetrieb nicht als *root*, sondern als nicht-privilegierter *user* an.
- Die Systemadministration findet über Netzwerk per UMS statt.
- Es können sich nicht mehrere nicht-privilegierte Nutzer gleichzeitig an OS 12 anmelden.

SYS.2.3.A2 Auswahl einer geeigneten Distribution (B)

- IGEL OS ist ein für sichere Arbeitsplätze gestaltetes Linux-Betriebssystem, dass sich umfassend managen lässt.
- IGEL versorgt eine Produktgeneration (z.B. IGEL OS 12, UMS 12) mindestens 3 Jahre mit Bug- und Security-Fixes sowie neuen Features. Bis 3 Jahre nach dem Verkaufsende einer Produktgeneration stellt IGEL noch Security-Fixes dafür zur Verfügung, siehe https://kb.igel.com/en/igel-subscription-and-more/current/igel-product-lifecycle. Derzeit hat IGEL noch keine Termine für End-of-Life (EOL) und End-of-Maintenance (EOM) für OS 12 und UMS 12 gesetzt.
- Die wichtigsten OS 12 Apps werden von IGEL paketiert, weitere Apps werden von IGEL-Partnern (IGEL Ready Developer) zur Verfügung gestellt und von IGEL einem Review unterzogen. Alle Apps werden von einem einzigen IGEL App Portal mittels sicheren Transfers bezogen.

SYS.2.3.A4 Kernel-Aktualisierungen auf unixartigen Systemen (B)

- Nach dem Einspielen eines System-Updates rebootet IGEL OS 12 automatisch.
- Daneben lassen sich Geräte von der UMS aus booten, bei Bedarf oder auch zeitgesteuert.

SYS.2.3.A5 Sichere Installation von Software-Paketen (B)

- Unter IGEL OS 12 wird Software nicht lokal aus dem Quelltext kompiliert. Apps werden als signierte Binärpakete installiert.

Weitere relevante Anforderungen

NET.1.1.A34 Einsatz kryptografischer Verfahren auf Netzebene (H)

- IEEE 802.1AE (MACsec) mit preshared Key ist in IGEL OS 12.3.0 und neuer unterstützt. Es lässt sich in **Netzwerk > LAN-Schnittstellen > Interface [Nummer] > MACsec** konfigurieren.

NET.2.1.A3 Auswahl geeigneter Kryptoverfahren für WLAN (B) [Planende]

- Verwenden Sie WPA2 Personal, WPA2 Enterprise oder WPA3 Personal für WLAN-Verbindungen.
- Wenn Sie WPA2 mit Pre-Shared Keys (WPA2-PSK) einsetzen, müssen Sie einen komplexen Schlüssel mit einer Mindestlänge von 20 Zeichen verwenden.

Parental Control Settings for IGEL OS

This article provides an overview of the settings that can be used for parental control in IGEL OS 12 and IGEL OS 11.

These settings can be controlled remotely from the IGEL Universal Management Suite (UMS) or locally on the device.

IGEL OS 12

(12.4.2-en) Password and User Types in IGEL OS 12

(12.4.2-en) Logon Settings in IGEL OS 12

(12.4.2-en) Change Password in IGEL OS 12

IGEL OS 11

(11.10.190-en) Password - Restrict Access to IGEL OS Components (contains information on the user types in IGEL OS 11)

(11.10.190-en) Security Logon

(11.10.190-en) Change Password

Xz Backdoor (CVE-2024-3094) Does Not Affect IGEL OS 11 and OS 12

IGEL OS 11 and IGEL OS 12 do not contain an xz package version that is vulnerable to the xz backdoor (CVE-2024-3094).
IGEL OS customers do not need to take any measures.
Customers running IGEL Universal Management Suite (UMS) on Linux or running IGEL Cloud Gateway (ICG) should check with their host OS vendor whether their OS version is vulnerable.

References

CVE-2024-3094: https://nvd.nist.gov/vuln/detail/CVE-2024-3094