intel

The latest security information on Intel® products.

Intel® PROSet/Wireless WiFi , Intel vPro® CSME WiFi and Killer™ WiFi Advisory

Intel ID:	INTEL-SA-00473
Advisory Category:	Firmware, Software
Impact of vulnerability:	Denial of Service
Severity rating:	MEDIUM
Original release:	05/11/2021
Last revised:	05/11/2021

Summary:

Potential security vulnerabilities in some Intel® PROSet/Wireless WiFi and Intel vPro® Converged Security and Management Engine (CSME) WiFi and Killer™ WiFi may allow denial of service. Intel is releasing firmware and software updates to mitigate these potential vulnerabilities.

Vulnerability Details:

CVEID: CVE-2020-24586 (Non-Intel issued)

Description: Fragment cache attack: A vulnerable device does not clear its cache/memory to remove fragments of an incomplete MSDU/MMPDU from previous session after reconnection/reassociation.

CVSS Base Score: 5.3 Medium

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

CVEID: CVE-2020-24587 (Non-Intel issued)

Description: Mixed key attack: A vulnerable device reassembles fragments encrypted under different keys in a protected network.

CVSS Base Score: 5.3 Medium

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

CVEID: CVE-2020-24588 (Non-Intel issued)

Description: Frame aggregation attack: Devices allow the encrypted payload to be parsed as containing one or more aggregated frames instead of a normal network packet.

CVSS Base Score: 5.3 Medium

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

Affected Products:

Intel® PROSet/Wireless WiFi products:

Intel® Wi-Fi 6E AX210

Intel® Wi-Fi 6 AX201

Intel® Wi-Fi 6 AX200

Intel® Wireless-AC 9560

Intel® Wireless-AC 9462

Intel® Wireless-AC 9461

Intel® Wireless-AC 9260

Intel® Dual Band Wireless-AC 8265

Intel® Dual Band Wireless-AC 8260

Intel® Dual Band Wireless-AC 3168

Intel® Wireless 7265 (Rev D) Family

Intel® Dual Band Wireless-AC 3165

Intel vPRO® CSME WiFi products:

Intel® Wi-Fi 6 AX201

Intel® Wi-Fi 6 AX200

Intel® Wireless-AC 9560

Intel® Wireless-AC 9260

Intel® Dual Band Wireless-AC 8265

Intel® Dual Band Wireless-AC 8260

Killer™ WiFi products:

Killer™ Wi-Fi 6E AX1675

Killer™ Wi-Fi 6 AX1650

Killer™ Wireless-AC 1550

Recommendations for Intel® PROSet/Wireless WiFi and Killer™ WiFi products:

Windows:

Intel recommends updating Intel® PROSet/Wireless WiFi to version 22.30 or later

Updates are available for download at this location:

https://downloadcenter.intel.com/download/30208

The 22.30.0 package installs the Windows 10 Wi-Fi drivers for the following Intel® Wireless Adapters:

- **22.30.0.11** for AX210/AX201/AX200/9560/9260/9462/9461 (Only available in 64-bit version)
- **20.70.21.2** for 8265/8260 (Only available in 64-bit version)
- **19.51.33.1** for 7265(Rev. D)/3165/3168

Intel recommends updating Killer™ WiFi to version 22.30.

Updates for Killer™ products are available for download at this location:

https://support.killernetworking.com

UEFI:

Intel recommends updating the WiFi drivers in UEFI to version 1.2.3-2121.

Please contact your OEM support group to obtain the correct driver version.

Chrome OS:

Intel® PROSet/Wireless WiFi drivers to mitigate these vulnerabilities will be up streamed to Chromium.

For any Google Chrome OS solution and schedule, please contact Google directly.

Linux OS:

Intel® PROSet/Wireless WiFi drivers to mitigate these vulnerabilities will be up streamed by March 9th, 2021.

Consult the regular Open Source channels to obtain this update.

Recommendation for Intel vPRO® CSME WiFi products:

Intel recommends updating Intel vPRO® CSME WiFi products to the following versions:

Processor	Chipset	Version	Device
10th Generation Intel® Core Processor Intel® Xeon® W Processor 10000/1200 Series	Intel® 400 Series Chipset	14.0.48	Intel® Wi-Fi 6 AX201 Intel® Wi-Fi 6 AX200
9th Generation Intel® Core Processor	Intel® 300 Series Chipset	12.0.72	Intel® Wireless-AC 9260 Intel® Wireless-AC 9560 Intel® Wi-Fi 6 AX200
8th Generation Intel® Core Processor	N/A	12.0.72	Intel® Wireless-AC 9260 Intel® Wireless-AC 9560 Intel® Wi-Fi 6 AX200
7th Generation Intel® Core Processor	Intel® 200 Series Chipset	11.8.83	Intel® Dual Band Wireless-AC 8265 Intel® Dual Band Wireless-AC 8260
6th Generation Intel® Core Processor	Intel® 100 Series Chipset		

Intel recommends that users of Intel® vPRO® CSME WiFi products update to the latest version provided by the system manufacturer that addresses these issues.

Acknowledgements:

These issues were found externally.

Intel, and nearly the entire technology industry, follows a disclosure practice called Coordinated Disclosure, under which a cybersecurity vulnerability is generally publicly disclosed only after mitigations are available.

Revision History

Revision	Date	Description
1.0	05/11/2021	Initial Release

Legal Notices and Disclaimers

Intel provides these materials as-is, with no express or implied warranties.

All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice.

Intel products and services described may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel products that have met their End of Servicing Updates may no longer receive functional and security updates. For additional details on support and servicing, please see this help article.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No product or component can be absolutely secure. Check with your system manufacturer or retailer or learn more at http://intel.com.

Some results have been estimated or simulated using internal Intel analysis or architecture simulation or modeling, and provided to you for informational purposes. Any differences in your system hardware, software or configuration may affect your actual performance.

Report a Vulnerability

If you have information about a security issue or vulnerability affecting an **Intel branded product or technology**, submit submit your report via the Intigriti platform, where you'll find eligibility criteria and submission instructions. All vulnerability reports must be submitted through Intigriti.

For issues not related to reporting security vulnerabilities, contact Intel PSIRT.

For issues related to Intel's external web presence (Intel.com and related subdomains), please contact Intel's External Security Research team.

Need product support?

If you...

- Have questions about the security features of an Intel product
- Require technical support
- Want product updates or patches

Please visit Support & Downloads.

Public Policy