

The latest security information on Intel® products.

[Report a Vulnerability](#) [Product Support](#)

Intel® PROSet/Wireless Wi-Fi Software and Intel® Wireless Bluetooth® Advisory

Intel ID:		INTEL-SA-01108	
Advisory Category:		Software	
Impact of vulnerability:		Denial of Service	
Severity rating:		MEDIUM	
Original release:		11/12/2024	

Intel ID:	INTEL-SA-01108
Last revised:	11/12/2024

Summary:

Potential security vulnerabilities in some Intel® PROSet/Wireless Software, Intel® Killer™ Wi-Fi and Intel® Wireless Bluetooth® may allow denial of service or information disclosure. Intel is releasing software updates to mitigate these potential vulnerabilities.

Vulnerability Details:

CVEID: CVE-2024-23198

Description: Improper input validation in firmware for some Intel® PROSet/Wireless Software and Intel® Killer™ Wi-Fi products before version 23.40 may allow an unauthenticated user to enable denial of service via adjacent access.

CVSS Base Score 3.1: 6.6 Medium

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

CVSS Base Score 4.0: 6.8 Medium

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

CVEID: CVE-2024-24984

Description: Improper input validation for some Intel® Wireless Bluetooth® products for Windows before version 23.40 may allow an unauthenticated user to potentially enable denial of service via adjacent access.

CVSS Base Score 3.1: 6.5 Medium

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

CVSS Base Score 4.0: 6.8 Medium

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

CVEID: CVE-2024-28049

Description: Improper input validation in firmware for some Intel® PROSet/Wireless Software and Intel® Killer™ Wi-Fi wireless products before version 23.40 may allow an unauthenticated user to enable denial of service via adjacent access.

CVSS Base Score 3.1: 5.7 Medium

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

CVSS Base Score 4.0: 6.8 Medium

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

CVEID: CVE-2024-25563

Description: Improper initialization in firmware for some Intel® PROSet/Wireless Software and Intel® Killer™ Wi-Fi before version 23.40 may allow a privileged user to potentially enable information disclosure via local access.

CVSS Base Score 3.1: 3.4 Low

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

CVSS Base Score 4.0: 4.6 Medium

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

Affected Products:

Intel® PROSet/Wireless Software, Intel® Killer™ Wi-Fi and Intel® Wireless Bluetooth® versions before 23.40 for:

- Intel® Wi-Fi 6 AX200
- Intel® Wi-Fi 6 AX201
- Intel® Wi-Fi 6E AX210
- Intel® Wi-Fi 6E AX211
- Intel® Wi-Fi 6E AX411
- Intel® Wireless-AC 9260
- Intel® Wireless-AC 9560
- Intel® Killer™ Wi-Fi 6 AX1650
- Intel® Killer™ Wi-Fi 6E AX1675
- Intel® Killer™ Wi-Fi 6E AX1690
- Intel® Wi-Fi 7 BE200
- Intel® Killer™ Wi-Fi 7 BE1750

Recommendation:

Intel recommends updating Intel® PROSet/Wireless Software, Intel® Killer™ Wi-Fi and Intel® Wireless Bluetooth® to version 23.40 or later.

Updates are available for download at this location:

Intel® Wireless Wi-Fi Drivers for Windows® 10 and Windows 11*

Intel® Wireless Bluetooth® Drivers for Windows® 10 and Windows 11*

Acknowledgements:

Intel would like to thank David Schögler for reporting CVE-2024-24984.

These issues were found internally by Intel employees CVE-2024-23198, CVE-2024-28049 and CVE-2024-25563.

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	11/12/2024	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.

© Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries United States and other countries. Other names and brands may be claimed as the property of others.

Report a Vulnerability

If you have information about a security issue or vulnerability with an **Intel branded product or technology**, please send an e-mail to secure@intel.com. Encrypt sensitive information using our [PGP public key](#).

Please provide as much information as possible, including:

- The products and versions affected
- Detailed description of the vulnerability
- Information on known exploits

A member of the Intel Product Security Team will review your e-mail and contact you to collaborate on resolving the issue. For more information on how Intel works to resolve security issues, see:

- [Vulnerability handling guidelines](#)

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](#).

[Company Overview](#)

[Contact Intel](#)

[Newsroom](#)

[Investors](#)

[Careers](#)

[Corporate Responsibility](#)

[Diversity & Inclusion](#)

[Public Policy](#)



© Intel Corporation

[Terms of Use](#)

[*Trademarks](#)

[Cookies](#)

[Privacy](#)

[Supply Chain Transparency](#)

[Site Map](#)

[Recycling](#)

