The latest security information on Intel® products.

Intel® Xeon® 6 processor E-Cores with Alias Checking Trusted Module Advisory

Intel ID:	**INTEL-SA-01273**
Advisory Category:	Firmware
Impact of vulnerability:	Escalation of Privilege
Severity rating:	HIGH
Original release:	05/13/2025
Last revised:	05/13/2025

Summary:

A potential security vulnerability in Alias Checking Trusted Module for some Intel® Xeon® 6 processor Efficient-Cores (E-Cores) may allow escalation of privilege. Intel is releasing firmware updates to mitigate this potential vulnerability.

Vulnerability Details:

CVEID: CVE-2025-20004

Description: Insufficient control flow management in the Alias Checking Trusted Module for some Intel® Xeon® 6 processor E-Cores firmware may allow a privileged user to potentially enable escalation of privilege via local access.

CVSS Base Score 3.1: 7.2 High

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

CVSS Base Score 4.0: 8.5 High

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

Affected Products:

Product Collection	Vertical Segment	CPU ID	Platform ID
Intel® Xeon® 6 Processor Family	Server	A06F0	0x01

Feedback

Recommendation:

Intel recommends that users of Intel® Xeon® 6 processor E-Cores with Alias Checking Trusted Module update to the latest version provided by the system manufacturer that addresses these issues.

Acknowledgements:

These following issue was found internally by Intel employees. Intel would like to thank Liron Shacham.

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	05/13/2025	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.

Feedback

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

Inclusion

Public Policy

Feedback

Terms of Use

*Trademarks

Cookies

Privacy

Supply Chain Transparency

Site Map

Recycling

Intel technologies may require enabled hardware, software or service activation. // No product or component can be absolutely secure. // Your costs and results may vary. // Performance varies by use, configuration, and other factors. Learn more at intel.com/performanceindex. // See our complete legal Notices and Disclaimers. // Intel is committed to respecting human rights and avoiding causing or contributing to adverse impacts on human rights. See Intel's Global Human Rights Principles. Intel's products and software are intended only to be used in applications that do not cause or contribute to adverse impacts on human rights.

intel

Feedback