intel.

The latest security information on Intel® products.

Intel® Trace Hub Advisory

Intel ID:	INTEL-SA-00609
Advisory Category:	Hardware
Impact of vulnerability:	Escalation of Privilege
Severity rating:	MEDIUM
Original release:	03/08/2022
Last revised:	04/08/2026

Summary:

A potential security vulnerability in some Intel® Trace Hub instances may allow escalation of privilege. Intel is releasing prescriptive guidance to address this potential vulnerability.

Vulnerability Details:

CVEID: CVE-2026-20709

Description: Use of Default Cryptographic Key in the hardware for some Intel® Pentium® Processor Silver Series, Intel® Celeron® Processor J Series, Intel® Celeron® Processor N Series may allow an escalation of privilege. Hardware reverse engineer adversary with a privileged user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via physical access when attack requirements are present with special internal knowledge and requires

no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (none) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (high), integrity (high) and availability (none) impacts.

CVSS Base Score 4.0: 5.8 Medium

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

CVSS Base Score 3.1: 6.6 Medium

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

CVEID: CVE-2021-33150

Description: Hardware allows activation of test or debug logic at runtime for some Intel(R) Trace Hub instances which may allow an unauthenticated user to potentially enable escalation of privilege via physical access.

CVSS Base Score 3.1: 5.3 Medium

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

Affected Products:

6th Gen Intel® Core™ Processors

7th Gen Intel® Core Processors

8th Gen Intel® Core™ Processors

10th Gen Intel® Core™ Processors

Intel Atom® processor A series

Intel Atom® processor C3000 Automated Driving series

Intel Atom® processor C3000 series

Intel Atom® processor X E3900 series

Intel® 100 series chipset

Intel® 200 series chipset

Intel® 300 series chipset

Intel® C230 series chipset

Intel® C240 series chipset

Intel® C420 chipset

Intel® C620 series chipset

Intel® Celeron® Processor 3000 Series (38XX and 39XX)

Intel® Celeron® Processor 4000 Series (42XX and 43XX)

Intel® Celeron® processor J3000/N3000 series

Intel® Celeron® processor J4000/N4000 series

Intel® Pentium® Gold Processor Series (44XX and 65XX)

Intel® Pentium® Gold Processor Series (54XX)

Intel® Pentium® Processor 4000 Series (44XX)

Intel® Pentium® processor J4000/N4000 series

Intel® Pentium® processor J5000/N5000 series

Intel® X299 chipset

Intel® Xeon® D processor 2000 series

Recommendations:

Intel is releasing prescriptive guidance to address this potential vulnerability and will not be providing additional mitigations for these chipset/SOC products. Intel recommends users follow existing security best practices and alternate security controls.

On April 01, 2026, Intel became aware of this issue through publicly available social media report that the researchers claims the extraction of Intel® SGX device specific key.

The issue only affects Intel® processors (codenamed: Gemini Lake) with Intel® SGX with CPUID 706A1, 706A8 specifically the following platforms:

- Intel® Celeron® Processor J Series
- Intel® Celeron® Processor N Series
- Intel® Pentium® Processor Silver Series

Please follow the same recommendations outlined below for both CVEs (CVE-2021-33150, CVE-2026-20709):

Intel recommends systems manufacturers follow the steps below to address this issue:

1. Setting up systems at the end of manufacturing to enable Intel® Firmware Version Control to help prevent this and other vulnerabilities.
2. Ensuring all security mitigations provided by Intel are applied and systems are running the latest firmware version available from Intel.
3. Following standard security practices and preventing unauthorized physical access to systems.

Additionally, Intel® SGX Provisioning Certification Service (Intel ® SGX PCS) will be updated to reference this security advisory. For more information refer to the security bulletin https://www.intel.com/content/www/us/en/security-center/announcement/intel-security-announcement-2026-04-08-001.html.

Some of the reported platforms have already reached End of Servicing Updates (ESU). Please review the following link for details on End of Servicing Updates platforms: https://www.intel.com/content/www/us/en/support/articles/000022396/processors.html

Acknowledgements:

CVE-2021-33150 was researched and reported by Mark Ermolov and Dmitry Sklyarov (Positive Technologies) and Maxim Goryachy (independent).

CVE-2026-20709 was researched by Mark Ermolov.

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	03/08/2022	Initial Release
1.1	04/08/2026	Updated new CVE-2026-20709

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 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.

Contact Intel

Newsroom

Investors

Careers

Corporate Responsibility

Inclusion

Public Policy

© Intel Corporation

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.

Skip to Main Content