The latest security information on Intel® products.

Intel® Processors MMIO Stale Data Advisory

Intel ID:	INTEL-SA-00615
Advisory Category:	Hardware
Impact of vulnerability:	Information Disclosure
Severity rating:	MEDIUM
Original release:	06/14/2022
Last revised:	06/27/2022

Summary:

Potential security vulnerabilities in Memory Mapped I/O (MMIO) for some Intel® Processors may allow information disclosure. Intel is releasing firmware updates to mitigate these potential vulnerabilities.

Vulnerability Details:

CVEID: CVE-2022-21123

Description: Incomplete cleanup of multi-core shared buffers for some Intel® Processors may allow an authenticated user to potentially enable information disclosure via local access.

CVSS Base Score: 6.1 Medium

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

CVEID: CVE-2022-21125

Description: Incomplete cleanup of microarchitectural fill buffers on some Intel® Processors may allow an authenticated user to potentially enable information disclosure via local access.

CVSS Base Score: 5.6 Medium

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

CVEID: CVE-2022-21127

Description: Incomplete cleanup in specific special register read operations for some Intel® Processors may allow an authenticated user to potentially enable information disclosure via local access.

CVSS Base Score: 5.5 Medium

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

CVEID: CVE-2022-21166

Description: Incomplete cleanup in specific special register write operations for some Intel® Processors may allow an authenticated user to potentially enable information disclosure via local access.

CVSS Base Score: 5.5 Medium

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

Affected Products:

Some Intel® Processors, see full list:

https://www.intel.com/content/www/us/en/developer/topic-technology/software-security-guidance/processors-affected-consolidated-product-cpu-model.html

Recommendations:

Intel recommends that users of the affected Intel® Processors update to the latest version provided by the system manufacturer that addresses these issues.

Intel® SGX PSW for Windows to version 2.16.100.3 or later:

https://registrationcenter.intel.com/en/products/download/3406/

Intel® SGX SDK for Windows to version 2.16.100.3 or later:

https://registrationcenter.intel.com/en/products/download/3407/

Intel® SGX DCAP for Windows to version 1.14.100.3 or later:

https://registrationcenter.intel.com/en/products/download/3610/

Intel® SGX PSW for Linux to version 2.17.100.3 or later:

https://01.org/intel-software-guard-extensions/downloads

Intel® SGX SDK for Linux to version 2.17.100.3 or later:

https://01.org/intel-software-guard-extensions/downloads

Intel® SGX DCAP for Linux to version 1.14.100.3 or later:

https://01.org/intel-software-guard-extensions/downloads

To address this issue, an Intel SGX TCB recovery is planned. Customers will require the microcode and software updates to get successful attestation responses. However, based on partner feedback and contingent on resolution of functional sightings impacting a subset of affected products, Intel is:

- Deferring the ability of the Development Environment (DEV) to enforce the presence of microcode and software updates on platforms via Intel® Enhanced Privacy ID (Intel® EPID) attestation to a future date, with the goal that this date be no later than March 7, 2023
- Deferring the ability of the Production Environment (LIV) to enforce the presence of microcode and software updates on platforms via Intel EPID attestation to a future date, with the goal that this date be no later than April 18, 2023
- For customers not using Intel EPID attestation, but are instead constructing their own attestation infrastructure using the Intel® SGX Provisioning Certification Service (Intel® SGX PCS), postponing the availability of new Endorsements / Reference Values (i.e. PCK Certificates and verification collateral) based on Intel Product Update 2022.1 / 3rd Generation Intel® Xeon® Scalable Processors, Codename IceLake-SP Post Launch Release 2 to a future date, with a goal that this date be no later than March 14, 2023. These customers decide when to enforce the microcode and software update, as part of their appraisal policies.

The functional sightings impacting a subset of affected products do not alter the effectiveness of the microcode and software provided to mitigate the above CVEs.

Refer to Intel SGX Attestation Technical Details

for more information on the Intel SGX TCB recovery process.

Further TCB Recovery Guidance

for developers is available

Acknowledgements:

The following issues were found internally by Intel employees. Intel would like to thank Ke Sun, Alan Miller, Shlomi Alkalay, Robert Jones, Ezra Caltum for reporting CVE-2022-21123, CVE-2022-21125, CVE-2022-21127, CVE-2022-21166. Jason Kilman for reporting CVE-2022-21123, CVE-2022-21127, and Scott Cape and Anthony Wojciechowski for reporting CVE-2022-21127.

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

Revision	Date	Description
1.0	06/14/2022	Initial Release
1.1	06/27/2022	Updated recommendations

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, processors, chipsets, and desktop boards 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 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 https://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 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

Report a Vulnerability Product Support

Please visit Support & Downloads .

Company Overview

Contact Intel

Newsroom

Investors

Careers

Corporate Responsibility

Diversity & Inclusion

Public Policy

Terms of Use

*Trademarks

Cookies

Privacy

Supply Chain Transparency

Site Map