The latest security information on Intel® products.

2022.1 IPU - Intel® Processor Advisory

Intel ID:	INTEL-SA-00617
Advisory Category:	Firmware
Impact of vulnerability:	Information Disclosure
Severity rating:	MEDIUM
Original release:	05/10/2022
Last revised:	06/13/2022

Summary:

A potential security vulnerability in some Intel® Processors may allow information disclosure. Intel is releasing firmware updates to mitigate this potential vulnerability.

Vulnerability Details:

CVEID: CVE-2022-21151

Description: Processor optimization removal or modification of security-critical code for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.

CVSS Base Score: 5.3 Medium

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

Affected Products:

Product Collection	Vertical Segment	CPU ID	Platform ID
10th Generation Intel® Core™ Processor Family	Mobile	706E5	80
Intel® Pentium® Processor Silver Series Intel® Celeron® Processor J Series Intel® Celeron® Processor N Series"	Desktop Mobile	706A1	01
8th Generation Intel® Core™ Processor Family	Desktop	906EB	02
8th Generation Intel® Core™ Processors	Mobile	806EC	94
10th Generation Intel® Core™ Processor Family	Desktop Mobile	A0653 A0655 AO661 806EC	22 02 80 94
6th Generation Intel® Core™ Processor Family	Desktop Mobile	506E3 406E3	36 C0
7th Generation Intel® Core™ Processor Family	Desktop Mobile	906E9 806E9	2A C0
9th Generation Intel® Core Processor Family	Desktop	A0671	02
3rd Generation Intel® Xeon® Scalable Processors	Server	606AX	0x87

Recommendations:

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

Intel has released microcode updates for the affected Intel® Processors that are currently supported on the public github repository. Please see details below on access to the microcode:

GitHub*: Public Github: https://github.com/intel/Intel-Linux-Processor-Microcode-Data-Files

This CVE requires a Microcode Security Version Number (SVN) update. To address this issue, an SGX TCB recovery is planned for Q2 2022. Customers will require the microcode update to get successful attestation responses. For customers using the Intel Attestation Service (IAS), the IAS Development Environment (DEV) will enforce the microcode and software updates beginning June 21, 2022 and the IAS Production Environment (LIV) will enforce the updates beginning July 19, 2022.

For customers that are not using IAS, but instead are constructing their own attestation infrastructure using the Intel® SGX Provisioning Certification Service (PCS), updated Endorsements/Reference Values (i.e., PCK Certificates and verification collateral) will be available June 28, 2022. These customers decide when to enforce the microcode and software update, as part of their Appraisal Policies.

Refer to Intel® SGX Attestation Technical Details for more information on the SGX TCB recovery process.

Further TCB Recovery Guidance for developers is available.

Acknowledgements:

This issue was found internally by Intel employees. Intel would like to thank Alysa Milburn, Jason Brandt, Avishai Redelman, Nir Lavi for reporting this issue.

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	05/10/2022	Initial Release
1.1	06/13/2022	Updated Recommendations

Legal Notices and Disclaimers

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 .