The latest security information on Intel® products.

2023.4 IPU Out-of-Band (OOB) - Intel® Processor Advisory

Intel ID:	INTEL-SA-00950
Advisory Category:	Hardware
Impact of vulnerability:	Escalation of Privilege, Denial of Service, Information Disclosure
Severity rating:	HIGH
Original release:	11/14/2023
Last revised:	11/14/2023

Summary:

A potential security vulnerability in some Intel® Processors may allow escalation of privilege and/or information disclosure and/or denial of service via local access. Intel is releasing firmware updates to mitigate this potential vulnerability.

Vulnerability Details:

CVEID: CVE-2023-23583

Description: Sequence of processor instructions leads to unexpected behavior for some Intel(R) Processors may allow an authenticated user to potentially enable escalation of privilege and/or information disclosure and/or denial of service via local access.

CVSS Base Score: 8.8 High

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

Affected Products:

Products with new microcode update:

Product Collection	Vertical Segment	CPU ID	Platform ID
10th Generation Intel® Core™ Processor Family	Mobile	706E5	80
3rd Generation Intel® Xeon® Processor Scalable Family	Server	606A6	87
Intel® Xeon® D Processor	Server	606C1	10
11th Generation Intel® Core Processor Family	Desktop Embedded	A0671	02
11th Generation Intel® Core Processor Family	Mobile Embedded	806C1 806C2 806D1	80 C2 C2
Intel® Server Processor	Server Embedded	A0671	02

The following products have already been mitigated:

Product Collection	Vertical Segment	CPU ID	Platform ID	Mitigated Microcode Version
12th Generation Intel® Core™ Processor Family	Mobile	906A4	80	0x2b
4th Generation Intel® Xeon® Processor Scalable Family	Server	806F8	87	0x2B000461
13th Generation Intel® Core™ Processor Family	Desktop	B0671	01	0x410E

For an exhaustive list of processors please visit:
https://www.intel.com/content/www/us/en/developer/topic-technology/software-security-guidance/processors-affected-consolidated-product-cpu-model.html

Recommendation:

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

Please refer to the technical paper here

for additional information.

Acknowledgements:

Intel would like to thank Intel employees: Benoit Morgan, Paul Grosen, Thais Moreira Hamasaki, Ke Sun, Alyssa Milburn, Hisham Shafi, and Nir Shlomovich for finding this issue internally.

Intel would like to thank Google Employees: Tavis Ormandy, Daniel Moghimi, Josh Eads, Salman Qazi, Alexandra Sandulescu, Andy Nguyen, Eduardo Vela, Doug Kwan, and Kostik Shtoyk for also 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	11/14/2023	Initial Release
1.1	11/14/2023	Updated recommendation technical paper link

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 Vulnerability Product Support 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 .