The latest security information on Intel® products.

Report a Vulnerability   Product Support

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

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 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

Diversity & Inclusion

Public Policy

© Intel Corporation

Terms of Use

*Trademarks

Cookies

Privacy

Supply Chain Transparency

Site Map

Do Not Share My Personal Information

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. // See our complete legal Notices and Disclaimers

. // Intel is committed to

respecting human rights and avoiding complicity in human rights abuses. 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 a violation of an internationally recognized human right.

intel.