The latest security information on Intel® products.

Intel® Server Boards, Server Systems and Compute Modules Advisory

Intel ID:	INTEL-SA-00434
Advisory Category:	Firmware
Impact of vulnerability:	Escalation of Privilege, Information Disclosure
Severity rating:	HIGH
Original release:	02/09/2021

Intel ID:	INTEL-SA-00434
Last revised:	02/09/2021

Summary:

Potential security vulnerabilities in some Intel® Server Boards, Server Systems and Compute Modules Baseboard Management Controller (BMC) firmware may allow escalation of privilege or information disclosure. Intel is releasing firmware updates to mitigate these potential vulnerabilities.

Vulnerability Details:

CVEID: CVE-2020-12374

Description: Buffer overflow in the BMC firmware for some Intel(R) Server Boards, Server Systems and Compute Modules before version 2.47 may allow a privileged user to potentially enable escalation of privilege via local access.

CVSS Base Score: 7.5 High

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

CVEID: CVE-2020-12377

Description: Insufficient input validation in the BMC firmware for some Intel(R) Server Boards, Server Systems and Compute Modules before version 2.47 may allow an authenticated user to potentially enable escalation of privilege via local access.

CVSS Base Score: 7.5 High

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

CVEID: CVE-2020-12380

Description: Out of bounds read in the BMC firmware for some Intel(R) Server Boards, Server Systems and Compute Modules before version 2.47 may allow an authenticated user to potentially enable escalation of privilege via local access.

CVSS Base Score: 6.5 Medium

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

CVEID: CVE-2020-12375

Description: Heap overflow in the BMC firmware for some Intel(R) Server Boards, Server Systems and Compute Modules before version 2.47 may allow an authenticated user to potentially enable escalation of privilege 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-2020-12376

Description: Use of hard-coded key in the BMC firmware for some Intel(R) Server Boards, Server Systems and Compute Modules before version 2.47 may allow authenticated user to potentially enable information disclosure via local access.

CVSS Base Score: 3.8 Low

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

Affected Products:

Intel® Server System R1000WF and R2000WF Families

Intel® Server Board S2600WF Family

Intel® Server Board S2600ST Family

Intel® Compute Module HNS2600BP Family

Intel® Server Board S2600BP Family

Recommendation:

Intel recommends updating the BMC firmware for the affected Intel® Server Boards, Server Systems, and Compute Modules to the latest version:

Intel® Server Systems and Server Board WF Family updates are available here

.

Intel® Server Board ST Family updates are available here

.

Intel® Compute Module and Server Board BP Family updates are available here

.

Acknowledgements:

The following issues were found internally by Intel employees. Intel would like to thank William Burton.

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	02/09/2021	Initial Release
1.1	02/18/2021	Fixed incorrect CVE assignment CVE-2020-12373 changed to 12374

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

Please visit Support & Downloads .

Company Overview

Contact Intel

Newsroom

Investors

Careers

Corporate Responsibility

Diversity & Inclusion

Public Policy