

Security Bulletin

Improper validation in BIOS firmware for some Intel Processors

Author(s) : Eviden PSIRT
Reference : PSIRT-744
Created : 16 January 2024
Version : 0.3
Status : Neutralization
TLP Classification : CLEAR
Document date : 14 March 2024
Keywords : CVE-2022-26006

TLP:CLEAR

Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

FOR PUBLIC USE

List of changes

Version	Date	Description
0.1	2024/01/19	Initial bulletin version
0.2	2024/02/15	TLP: CLEAR
0.3	2024/03/14	Removal of ambiguous sentence: no patch effort is undergoing.

Executive summary

A flaw in Intel processors may allow a privileged user to potentially enable escalation of privilege via local access.

This vulnerability affects some servers of the BullSequana XH1000 family. No patch will be made available as the corresponding CPU architecture is out of support.

Vulnerability Info

CVE No.	CVSS Score	Type of Vulnerability
CVE-2022-26006	6.7	CWE-20 Improper Input Validation CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVE-2022-26006 - The BIOS Firmware does not properly validate data that is being referenced by an SMI handler. This may lead to an incorrect size calculation when checking the location of input buffers allowing memory operations outside the intended buffer boundary.

Affected products

The products are affected according to the precise versions of processor embedded. The Intel processors report their precise version through the CPUID instruction.

Windows operating systems

Follow [Intel's instruction](#) to get your CPUID. The CPUID is part of the processor ID.

```

Select Command Prompt - wmic
C:\>wmic
wmic:root\cli>cpu get processorid
ProcessorId
BFEBFBFF0000806EC
    
```

Linux operating systems

To obtain the CPUID of your Intel CPU, use the following command.

```

lscpu | awk '\
($1 == "Model:") {m1=$2/16; m2=$2%16}\
($1 == "Stepping:") {step=$2}\
($1 " " $2 == "CPU family:") {family=$3}\
END {printf("%.1x%.2x%.1x%.1x\n", m1, family, m2, step)} '
    
```

```

$ lscpu | awk '\
($1 == "Model:") {m1=$2/16; m2=$2%16}\
($1 == "Stepping:") {step=$2}\
($1 " " $2 == "CPU family:") {family=$3}\
END {printf("%.1x%.2x%.1x%.1x\n", m1, family, m2, step)} '
806ec
$
    
```

List of affected CPUID

The reference for affected CPUID is Intel's [consolidated list of affected processors](#). The affected CPUID that you may find in BullSequana platforms are of the following type:

Component name	CPUID	Comments
Haswell EP	306F2	This product has met Intel's End of Servicing Updates (ESU)
Broadwell EP	406F1	This product has met Intel's End of Servicing Updates (ESU)

List of Enterprise and Edge servers

BullSequana Edge servers are not affected.

CPUID	BullionS
306F2	Unpatched
406F1	Unpatched

List of HPC products

BullSequana X400, X800, X2000, and X3000 series are not affected.

The table below provides the Technical State to apply to implement Intel mitigation measures.

CPUID	BullxR400-E4	Bullx S6010	Bullx DLC B720	BullSequana X1110
306F2	Unpatched	Unpatched	Unpatched	Unpatched
406F1	Unpatched	Unpatched	Unpatched	Unpatched

Disclaimer

Although Eviden makes effort to provide accurate and complete information, Eviden shall not be liable if the above tables are incomplete or erroneous. During its vulnerability analysis process, the information in this document is subject to change without notice to reflect new results of this analysis.

TS (technical state) with no number indicates that a new technical state fixing the vulnerabilities is scheduled.

TBD (to be defined) indicates that a new technical state fixing the vulnerabilities is under study.

Unpatched means that the vulnerability is presumably present, but there is no plan to provide a fix. This can be investigated on demand.

Recommendations

Eviden recommends applying its Technical States upgrade on its servers as soon as they are made available.

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

Available Vendor Patches

No validated patch is available at the time.

Technical States links for Eviden servers are reminded in the table below.

Product	Technical State link
Bullion S	https://support.bull.com/ols/product/platforms/bullion/bullion-S/dl/pkgf/pkg
Bullx DLC	https://support.bull.com/ols/product/platforms/hw-extremcomp/bullx_dlc/bullx_b720
Bull Sequana X1000	https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x1000/dl/pkgf/pkg

Available Workarounds

No workaround is available.

Available Mitigations

No mitigation identified.

Available Exploits/PoC

Eviden is not aware of any exploitation of the reported vulnerabilities.

References

1. <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00688.html>
2. <https://nvd.nist.gov/vuln/detail/CVE-2022-26006>

Glossary of terms

Term	Description
Mitigation	Refers to a setting, common configuration, or general best-practice, existing in a default state that could reduce the severity of exploitation of a vulnerability
Neutralization	The neutralization phase is the decision-making process during which the risk posed by an incident is evaluated.
PoC	Proof of Concept
Remediation	The remediation phase ends with the delivering of a qualified solution/update fixing the vulnerability without regression.
TI	Threat Intelligence
TLP	Traffic Light Protocol (TLP) FIRST Standards Definitions and Usage Guidance — Version 2.0. https://www.first.org/tlp/
Workaround	Refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update

About this document

Eviden continuously monitors the security of its products. This Security Bulletin is shared under the constraints of the FIRST Traffic Light Protocol version 2.0 (TLP) to bring attention of owners of the potentially affected Eviden products. Eviden recommends that all product owners determine whether the described situation is applicable to their individual case and take appropriate action.

Although Eviden makes effort to provide accurate and complete information, Eviden shall not be liable for technical or editorial errors contained in this Bulletin. The information provided is provided “as is” without warranty of any kind. To the extent permitted by the Law, neither Eviden nor its affiliates, subcontractors or suppliers will be liable for incidental damages, downtime cost, lost profits, damages relating to the procurement of substitute products or services, or damages for loss of data, or software restoration. Product and company names mentioned herein may be trademarks of their respective owners.

The information in this document is subject to change without notice. The version of this document will be incremented according to the changes:

- Neutralization security bulletins are numbered 0.x
- Privately disclosed Remediation security bulletins are numbered 1.x
- Publicly disclosed Remediation security bulletins are numbered 2.x

Updated versions of this document can be found on:

- <https://support.bull.com/ols/product/security/psirt>

About Atos

Atos is a global leader in digital transformation with 105,000 employees and annual revenue of c. € 11 billion. European number one in cybersecurity, cloud and high-performance computing, the Group provides tailored end-to-end solutions for all industries in 69 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The [purpose of Atos](#) is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

About Eviden¹

[Eviden](#) is a next-gen technology leader in data-driven, trusted and sustainable digital transformation with a strong portfolio of patented technologies. With worldwide leading positions in advanced computing, security, AI, cloud and digital platforms, it provides deep expertise for all industries in more than 47 countries. Bringing together 53,000 world-class talents, Eviden expands the possibilities of data and technology across the digital continuum, now and for generations to come. Eviden is an Atos Group company with an annual revenue of c. € 5 billion.

¹ Eviden business is operated through the following brands: AppCentrica, ATHEA, Cloudamize, Cloudreach, Cryptovision, DataSentics, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, In Fidem, Ipsotek, Maven Wave, Profit4SF, SEC Consult, Visual BI, Worldgrid, X-Perion. Eviden is a registered trademark. © Eviden SAS, 2023.