EVIDEN
an atos business

Security Bulletin

Multiple vulnerabilities fixed in BullSequana platforms Mesca3

Author(s)	:	**Eviden PSIRT**
Reference	:	**PSIRT-736**
Created	:	**27 February 2024**
Version	:	**2.7**
Status	:	**Remediation**
TLP Classification	:	**CLEAR**
Document date	:	**19 July 2024**
Keywords	:	**CVE-2003-0001 CVE-2015-3200 CVE-2018-19052 CVE-2018-25183 CVE-2019-11072 CVE-2021-36369 CVE-2022-01292 CVE-2022-21166 CVE-2022-22707 CVE-2022-30780 CVE-2022-37797 CVE-2022-40982 CVE-2022-41556 CVE-2023-00464 CVE-2023-02650 CVE-2023-03446 CVE-2023-03817 CVE-2023-04807 CVE-2023-48795 CVE-2023-48795**

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
1.0	2024/02/09	Initial remediation version
1.1	2024/02/27	CVE-2023-48795 added to bulletin. Vulnerabilities added CVE-2018-19052, CVE-2019-11072, CVE-2022-22707, CVE-202230780, CVE-2022-37797, CVE-2022-41556 – lighttpd, CVE-2023-48795 – dropbear
1.2	2024/03/12	Title change. TS number change. Adding CVE-2021-36369. Removing CVE-2023-48795. Removing table duplicates.
1.3	2024/03/14	Clarifying status for CVE-2021-36369, CVE-2023-4807, and.CVE-2023-48795. Adding CVE-2022-21166. Adding note to remind performance issues with CVE-2022-40982 fix.
1.4	2024/04/03	Adding CVE-2003-0001 and CVE-2015-3200
1.5	2024/05/03	Adding mention of dropbear 2024.84 fixing CVE-2023-48795
2.6	2024/06/28	TLP changed for CLEAR
2.7	2024/07/19	Added information about vulnerabilities in iCare, added CVE-2018-25103

Executive summary

This bulletin covers vulnerabilities fixed in a new technical state (TS 74) for Mesca3 based platforms. It is prepared to support delivery of this new TS.

The fixed vulnerabilities are found in Enterprise products BullSequana M, BullSequana S and HPC products Atos QLM, BullSequana X800. They are related to the BMC (web interface security) and the BIOS (security fixes and Intel microcode updates).

Eviden reminds that the iCare product suffers critical vulnerabilities and is declared end-of-support (see bulletin).

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

Vulnerability Info

Vulnerabilities affecting the BMC

CVE No.	CVSS Score	Type of Vulnerability
CVE-2003-0001	5.2	Etherleak
CVE-2015-3200	7.5	lighttpd
CVE-2018-19052	7.5	lighttpd
CVE-2018-25103	5.3	lighttpd
CVE-2019-11072	9.8	lighttpd
CVE-2021-36369	N/A	Dropbear; Only applies to dropbear as a client
CVE-2022-1292	9.8	openssl: c_rehash script allows command injection

CVE-2022-22707	5.9	lighttpd
CVE-2022-30780	7.5	lighttpd
CVE-2022-37797	7.5	lighttpd
CVE-2022-41556	7.5	lighttpd
CVE-2023-0464	7.5	openssl: Denial of service by excessive resource usage in verifying X509 policy constraints
CVE-2023-2650	6.5	openssl: Possible DoS translating ASN.1 object identifiers
CVE-2023-3446	5.3	openssl: Excessive time spent checking DH keys and parameters
CVE-2023-3817	5.3	openssl: Excessive time spent checking DH q parameter value
CVE-2023-4807	N/A	openssl: POLY1305 MAC implementation corrupts XMM registers on Windows. Not applicable to BMC.
CVE-2023-48795	3.0	Dropbear: terrapin weakness

Vulnerabilities affecting the OS (through BIOS)

CVE No.	CVSS Score	Type of Vulnerability
CVE-2022-21166	5.5	Incomplete cleanup in specific special register write operations for some Intel® Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2022-40982	6.5	Intel DownFall CWE-203 Observable Discrepancy CWE-1342 Information Exposure through Microarchitectural State after Transient Execution

Vulnerabilities affecting the iCare management suite

The iCare management suite was part of Mesca3 Technical states. All iCare versions are subject to the following critical vulnerabilities. The product iCare is declared end-of-Support.

CVE No.	CVSS Score	Type of Vulnerability
CVE-2024-TBD	10	Authorization Bypass Local Privilege Escalation Remote Command Execution AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Affected products

Products	Fixed version	Status	Comments
BullSequana M BullSequana S Atos QLM BullSequana X800	TS 74.01	Fixed	Fixed vulnerabilities: CVE-2015-3200, CVE-2018-19052, CVE-2019-11072, CVE-2022-1292, CVE-2022-21166, CVE-2022-22707, CVE-2022-30780, CVE-2022-37797, CVE-2022-40982, CVE-2022-41556, CVE-2023-0464, CVE-2023-2650, CVE-2023-3446, CVE-2023-3817, CVE-2023-48795

Notes:

1. The vulnerabilities CVE-2021-36369 and CVE-2023-4807 are not listed in the above table since they are not considered as affecting the platforms. Yet, this TS incorporates a patch level fixing them.
2. CVE-2022-40982: Eviden recommends using the OS option to turn off mitigation by default and carefully test the performance impact before activation of the mitigation in production (see Eviden's advisory about GDS Vulnerability in Intel).
3. CVE-2003-0001 was discovered lately as affecting the Ethernet NIC device driver. See dedicated bulletin for details.
4. CVE-2018-25103 was disclosed after TS elaboration. Yet, it is fixed as lighttpd version is 1.4.74 > 1.4.50.

Although Eviden makes effort to provide accurate and complete information, Eviden shall not be liable if the above table is 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.

Available Vendor Patches

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

Product	Technical State link
Bull Sequana S	https://support.bull.com/ols/product/platforms/bullion/bullsequana-s/dl/pkgf/technical-state-dvd-packages
Bull Sequana X800 / QLM	https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x800/dl/pkgf/pkg

Available Exploits/PoC

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

References

1. https://nvd.nist.gov/vuln/detail/CVE-2022-1292
2. https://www.openssl.org/news/secadv/20220503.txt
3. https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=e5fd1728ef4c7a5bf7c7a7163ca60370460a6e23
4. https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=548d3f280a6e737673f5b61fce24bb100108dfeb
5. https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=1ad73b4d27bd8c1b369a3cd453681d3a4f1bb9b2
6. https://nvd.nist.gov/vuln/detail/CVE-2023-0464
7. https://www.openssl.org/news/secadv/20230322.txt
8. https://nvd.nist.gov/vuln/detail/CVE-2023-0464
9. https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=2017771e2db3e2b96f89bbe8766c3209f6a99545
10. https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=879f7080d7e141f415c79eaa3a8ac4a3dad0348b
11. https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=959c59c7a0164117e7f8366466a32bb1f8d77ff1
12. https://nvd.nist.gov/vuln/detail/CVE-2023-3446
13. https://www.openssl.org/news/secadv/20230719.txt
14. https://www.openwall.com/lists/oss-security/2023/07/31/1
15. https://nvd.nist.gov/vuln/detail/CVE-2023-3817
16. https://www.openssl.org/news/secadv/20230731.txt
17. https://nvd.nist.gov/vuln/detail/CVE-2023-4807
18. https://www.openssl.org/news/secadv/20230908.txt
19. https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00615.html
20. https://support.bull.com/ols/product/security/psirt/security-bulletins/gds-vulnerability-in-intel-advisory-psirt-535-tlp-clear-version-2-9-cve-2022-40982/at_download/file
21. https://support.bull.com/ols/product/security/psirt/security-bulletins/ethernet-frame-padding-information-leakage-etherleak-psirt-1169-tlp-green-version-0-1-cve-2003-0001/at_download/file

22. https://kb.cert.org/vuls/id/312260
23. https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security%20Advisories/2024/AMI-SA-2024002.pdf
24. https://blogvdoo.wordpress.com/2018/11/06/giving-back-securing-open-source-iot-projects/#more-736
25.

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 provides 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 Eviden[1]

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.