EVIDEN
an atos business

Security Bulletin

Ethernet leakage on some BullSequana BMCs

Author(s)	:	**Eviden PSIRT**
Reference	:	**PSIRT-1169**
Created	:	**21 March 2024**
Version	:	**0.2**
Status	:	**Neutralization**
TLP Classification	:	**CLEAR**
Document date	:	**28 June 2024**
Keywords	:	**CVE-2003-0001**

TLP:GREEN

Limited disclosure, recipients can spread this within their community. Eviden may use TLP:GREEN when information is useful to increase awareness within the cybersecurity community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community.

RESTRICTED SHARING - FOR EXTERNAL USE

List of changes

Version	Date	Description
0.1	2024/03/23	Initial neutralization bulletin
0.2	2024/06/28	TLP:CLEAR

Executive summary

It has been reported that some security scanners detect "Non-Zero Padding Bytes Observed in ICMP Protocol Unreachable Packets" when scanning the BMC of some BullSequana servers. This vulnerability was first reported as CVE-2003-0001 and named Etherleak.

Since 2003, the vulnerable NIC linux drivers have likely been patched. Yet, this vulnerability pops up regularly ever since (see for instance CVE-2017-2304). This is due to the uncertainty of the detection method and its influenceability by other network devices (see for instance this IBM advisory).

Nevertheless, the Eviden BDS PSIRT has independently confirmed that the security scanners reports are not false positive in the case of Mesca 3 platform. This does not affect more recent platforms. It is likely due to some out-of-support proprietary NIC driver. Eviden is liaising closely with its suppliers and investigating the exact nature of these vulnerabilities to provide validated remediation.

Despite being vulnerable, the Eviden BDS PSIRT assesses that there is no significant risk in this weakness. In the context of a BMC, no scenario could lead to the leak of interesting data. The recovered data is not controllable and totally independent from any communication from the CPUs.

Vulnerability Info

CVE No.	CVSS Score	Type of Vulnerability
CVE-2003-0001	5.2	CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor

At the time the vulnerability was discovered, many ethernet Network Interface Card (NIC) device drivers did not properly pad frames with null bytes, leaving them susceptible to exploitation by remote attackers who can retrieve information from previous packets or kernel memory using malformed packets. This was nicknamed “Etherleak”.

Network device drivers often utilize outdated frame buffer data to fill packets, creating a security flaw that could potentially enable malicious actors to extract confidential information from vulnerable devices.

The Ethernet standard, also known as IEEE 802.3, mandates a minimum data field size of 46 bytes. In cases where a higher layer protocol like IP supplies packet data smaller than 46 bytes, the device driver is required to fill the remaining space in the

data field with a "pad". RFC1042, which pertains to IP datagrams, states that the data field should be padded with zero octets to satisfy the minimum frame size requirements of IEEE 802.

Researchers uncovered that many Ethernet device drivers do not adhere to the recommendations of RFC1042. Instead of padding frames with null bytes, these drivers recycle data from previously sent frames to pad frames smaller than 46 bytes. This flaw introduces a vulnerability for information leakage, potentially allowing remote attackers to access sensitive information. The leaked data could originate from dynamic kernel memory, static system memory allocated to the device driver, or a hardware buffer on the network interface card.

Remote attackers can exploit this vulnerability to gather potentially sensitive data from network transmissions. Additionally, in specific network configurations, this flaw can be leveraged to evade security protocols that segment networks into isolated domains, such as VLANs and routers.

Application to Mesca3 platforms

In the case of the Mesca3 BMC, it has been confirmed that the padding is incorrectly non-zero. The retrieved information, however, doesn't seem to pose any risk as it is not controllable by the opponent.

Affected products

Products	Fixed version	Status	Comments
BullSequana M BullSequana S QLM BullSequana X800	TBD	Affected	

Although Eviden tries 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

No validated patch is available at this time. Eviden is working with its suppliers to distribute updates as soon as possible.

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 Workarounds

No workarounds available.

Available Mitigations

The BMC should not be exposed to other networks than the management one.

Exploiting the vulnerability implies port knocking activity which is highly detectable.

Available Exploits/PoC

An exploit script is publicly available. Eviden is not aware of any practical exploitation of this vulnerability.

References

1. https://github.com/advisories/GHSA-945x-53jf-h5qf
2. https://nvd.nist.gov/vuln/detail/CVE-2003-0001
3. https://nvd.nist.gov/vuln/detail/CVE-2017-2304
4. https://www.kb.cert.org/vuls/id/412115
5. https://access.redhat.com/solutions/875043
6. https://www.ibm.com/support/pages/ibm-aix-my-system-vulnerable-etherleak-cve-2003-0001
7. https://community.ui.com/questions/EtherLeak-on-Edge-Router-x-CVE-2017-2304/c26844e8-4efd-4fa4-b56b-558dc5f5043c
8. https://www.exploit-db.com/exploits/3555

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 the 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 tries to provide accurate and complete information, Eviden shall not be liable for technical or editorial errors contained in this Bulletin. The information 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.