EVIDEN
an atos business

Security Bulletin

TLS Protocol Session Renegotiation Vulnerability

Author(s)	:	**Eviden PSIRT**
Reference	:	**PSIRT-646**
Created	:	**23 November 2023**
Version	:	**2.3**
Status	:	**Remediation**
TLP Classification	:	**CLEAR**
Document date	:	**3 May 2024**
Keywords	:	**CVE-2009-3555**

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	2023/12/22	Initial Eviden bulletin
1.2	2024/04/05	Workaround proposed
2.3	2024/05/03	TLP:CLEAR version. Mention of Bullion S EOL/EOS.

Executive summary

The BMCs of Bullion S and BullSequana S servers, if left in their original configuration, allow usage of vulnerable SSL or TLS protocols. Usual vulnerability scanners can be used to detect the misconfiguration.

Vulnerability Info

CVE No.	CVSS Score	Type of Vulnerability
CVE-2009-3555	N/A	CWE-295 Improper Certificate Validation

The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a "plaintext injection" attack, aka the "Project Mogul" issue.

Testing TLS/SSL configuration using Nmap.

The **ssl-enum-ciphers** script in Nmap is designed to detect the cipher suites supported by a server and evaluate their cryptographic strength. It establishes connections using SSLv3, TLS 1.1, and TLS 1.2 protocols. Additionally, the script alerts if it detects any vulnerabilities in the SSL implementation, including known issues like crime and poodle.

As an example, a Bullion S platform may present the following ciphers:

```
[root@admintools ~]# nmap -sV --script ssl-enum-ciphers  10.197.180.26

Starting Nmap 6.40 ( http://nmap.org ) at 2023-12-13 16:47 CET
Nmap scan report for s8-pvt-bmc0.frec.bull.fr (10.197.180.26)
Host is up (0.00058s latency).
Not shown: 995 closed ports
```

```
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      Dropbear sshd 0.45 (protocol 2.0)
23/tcp  open  telnet   Cisco or Edge-core switch telnetd
24/tcp  open  telnet   Busybox telnetd
80/tcp  open  http     Supermicro IPMI/Paradox Alarm http config
443/tcp open  ssl/http Supermicro IPMI/Paradox Alarm http config
| ssl-enum-ciphers:
|   SSLv3:
|     ciphers:
|       TLS_RSA_EXPORT_WITH_DES40_CBC_SHA - weak
|       TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 - weak
|       TLS_RSA_EXPORT_WITH_RC4_40_MD5 - weak
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_DES_CBC_SHA - weak
|       TLS_RSA_WITH_RC4_128_MD5 - strong
|       TLS_RSA_WITH_RC4_128_SHA - strong
|     compressors:
|       NULL
|   TLSv1.0:
|     ciphers:
|       TLS_RSA_EXPORT_WITH_DES40_CBC_SHA - weak
|       TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 - weak
|       TLS_RSA_EXPORT_WITH_RC4_40_MD5 - weak
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_DES_CBC_SHA - weak
|       TLS_RSA_WITH_RC4_128_MD5 - strong
|       TLS_RSA_WITH_RC4_128_SHA - strong
|     compressors:
|       NULL
|_  least strength: weak
MAC Address: 08:00:38:3C:EA:90 (Bulls.)
Service Info: Host: 10.197.180.26; OS: Linux; Devices: switch, remote
management; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 62.14 seconds
```

Affected products

Products	Fixed version	Status	Comments
Bullion S – Mesca2	TS 26.03	Fixed	This product is out-of-support, but the latest TS configures the TLS 1.2 protocol for the BMC.
BullSequana S – Mesca3	TS 64.01	Fixed	This TS introduces a configuration setting which is accessible through BSMCLI (see Workaround). To run BSMCLI with TS64, it is necessary to use BSMHW_NG version 1.5.31 (Available on Tools Downloads)

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

Apply the latest TS and proper configuration.

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
Bullion S	https://support.bull.com/ols/product/platforms/bullion/bullion-S/dl/pkgf/pkg-orig

Available Workarounds

For BullSequana S, the TS64.01 deactivates SSLv3 and only accepts TLS. A specific parameter exists to restrict the TLS protocol versions: bmc.tls_version.

The possible values are:

0. Minimum version is TLS 1.0 (no restriction)
1. Minimum version is TLS 1.1
2. Minimum version is TLS 1.2
3. Minimum version is TLS 1.3

Use BSMCli tool to set the parameter to the desired value (TLS 1.3 in the below example).

```
/opt/BSMHW_NG/sbin/ipmi-oem -h <server> -u <user> -p <password> \
bull setcfg bmc.tls_version 3
```

Make sure that the tools used to access the BMC support the desired protocol before setting the parameter.

Available Mitigations

Ensure that all remote server management interfaces (e.g. Redfish, IPMI) and BMC subsystems in their environments are on their dedicated management networks and are not exposed externally and ensure internal BMC interface access is restricted to administrative users with ACLs or firewalls.

Available Exploits/PoC

Eviden is not aware of any exploitation of the reported vulnerabilities in the context of its servers.

References

1. https://nvd.nist.gov/vuln/detail/CVE-2009-3555
2. https://access.redhat.com/articles/20490

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.