EVIDEN
an atos business

Security Bulletin

RCE Vulnerability in OpenSSH server - regreSSHion

Author(s)	:	Eviden PSIRT
Reference	:	PSIRT-1395
Created	:	02 July 2024
Version	:	0.2
Status	:	Neutralization
TLP Classification	:	CLEAR
Document date	:	12 July 2024
Keywords	:	CVE-2024-6387 CVE-2024-6409

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	2024/07/02	Initial bulletin version
0.2	2024/07/12	CVE-2024-6409 added to bulletin

Executive summary

A Remote Unauthenticated Code Execution (RCE) vulnerability in OpenSSH's server (sshd) has been uncovered by the Qualys Threat Research Unit (TRU) on glibc-based Linux systems.

The CVE assigned to this vulnerability is CVE-2024-6387.

OpenSSH's server (sshd) on glibc-based Linux systems is susceptible to a signal handler race condition, leading to unauthenticated remote code execution (RCE) as root. This vulnerability presents a significant security risk, especially given its impact on sshd's default configuration.

This vulnerability does not affect Eviden servers baseboard management controllers (BMC).

Exploitaton against the host part of Eviden servers (AMD or Intel CPUs) remains difficult.

For HPCs, RHEL 7 and RHEL 8 do not embed a vulnerable version of openssh. For RHEL 9 RedHat published fix

CVE-2024-6409 - a signal handler race condition vulnerability was found in OpenSSH's server (sshd), where a client does not authenticate within LoginGraceTime seconds (120 by default, 600 in old OpenSSH versions), then sshd's SIGALRM handler is called asynchronously. However, this signal handler calls various functions that are not async-signal-safe, for example, syslog(). This issue leaves it vulnerable to a signal handler race condition on the cleanup_exit() function, which introduces the same vulnerability as CVE-2024-6387 in the unprivileged child of the SSHD server.

Vulnerability Info

The root cause of this vulnerability was introduced in October 2020 (OpenSSH 8.5p1), as a regression of the previously patched CVE-2006-5051 vulnerability has been identified.

Affected Versions: 8.5p1 <= OpenSSH < 9.8p1

Qualys researchers have managed to exploit this vulnerability on 32-bit (i386) Linux systems and achieve code execution with root privileges. According to their report, it usually requires approximately 10,000 attempts to succeed and about a week to obtain a root shell. The 64bit (amd64) architecture will pose a greater challenge for exploitation due to enhanced ASLR and enforced NX bits.

CVE No.	CVSS Score	Type of Vulnerability
CVE-2024-6387	7.1	CWE-364 Signal Handler Race Condition AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:W/RC:R
CVE-2024-6409	7.0	CWE-364 Signal Handler Race Condition AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:H

Eviden is liaising closely with its suppliers and investigating the exact nature of these vulnerabilities to provide validated remediation.

Affected products

Products	Fixed version	Status	Comments
OpenSSH	9.8p1	Fixed	https://www.openssh.com/releasenotes.html#9.8p1

Recommendations

Eviden recommends applying openssh patches as soon as they are made available by distribution vendors.

Available Vendor Patches

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

For HPC infrastructure, RedHat is planning to publish patch for the affected components:

Component	RHEL 7	RHEL 8	RHEL 8.6 EUS	RHEL 8.8 EUS	RHEL 9
Openssh CVE-2024-6387	Not Affected	Not Affected	Not Affected	Not Affected	Fixed RHSA-2024:4312
CVE-2024-6409	Not Affected	Not Affected	Not Affected	Not Affected	Fixed RHSA-2024:4457

Available Workarounds

Red Hat is proposing the following workaround waiting for the official fix

This issue can be mitigated by setting the LoginGraceTime parameter to 0 in the sshd configuration file.

1) As root user, open the `/etc/ssh/sshd_config`
2) Add or edit the parameter configuration:

```
LoginGraceTime 0
```

3) Save and close the file
4) Restart the sshd daemon:

```
systemctl restart sshd.service
```

Available Mitigations

The exploitation of the vulnerability against nodes running 64bits glibc is unconfirmed. As for any race condition attack, traces in logs are easy to detect.

Available Exploits/PoC

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

References

1. https://www.qualys.com/2024/07/01/cve-2024-6387/regresshion.txt
2. https://access.redhat.com/security/cve/CVE-2024-6387
3. https://nvd.nist.gov/vuln/detail/CVE-2024-6387
4. http://www.openwall.com/lists/oss-security/2024/07/01/12
5. http://www.openwall.com/lists/oss-security/2024/07/01/13
6. https://www.openssh.com/txt/release-9.8
7. https://access.redhat.com/errata/RHSA-2024:4312
8. https://access.redhat.com/errata/RHSA-2024:4389
9. https://access.redhat.com/errata/RHSA-2024:4340
10. http://www.openwall.com/lists/oss-security/2024/07/11/3
11. https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server
12. https://forum.vmssoftware.com/viewtopic.php?f=8&t=9132
13. https://arstechnica.com/security/2024/07/regresshion-vulnerability-in-openssh-gives-attackers-root-on-linux/
14. https://access.redhat.com/security/cve/CVE-2024-6409
15. https://access.redhat.com/errata/RHSA-2024:4457
16. http://www.openwall.com/lists/oss-security/2024/07/08/2
17. http://www.openwall.com/lists/oss-security/2024/07/09/2
18. http://www.openwall.com/lists/oss-security/2024/07/09/5
19. http://www.openwall.com/lists/oss-security/2024/07/10/1
20. http://www.openwall.com/lists/oss-security/2024/07/10/2
21. https://bugzilla.redhat.com/show_bug.cgi?id=2295085
22. https://bugzilla.suse.com/show_bug.cgi?id=1227217

23. https://explore.alas.aws.amazon.com/CVE-2024-6409.html
24. https://github.com/openela-main/openssh/commit/c00da7741d42029e49047dd89e266d91dcfbffa0
25. https://security-tracker.debian.org/tracker/CVE-2024-6409
26. https://sig-security.rocky.page/issues/CVE-2024-6409

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, BullSequana, Cloudamize, Cloudreach, Cryptovision, DataSentics, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, IDnomic, In Fidem, Ipsotek, Maven Wave, Profit4SF, SEC Consult, Trustway, Visual BI, Worldgrid, X-Perion.