Security Bulletin

Vulnerabilities in Netfilter

Author(s)	:	Eviden PSIRT
Reference	:	PSIRT-1180
Created	:	07 June 2024
Version	:	2.2
Status	:	Remediation
TLP Classification	:	CLEAR
Document date	:	14 June 2024
Keywords	:	CVE-2023-3390, CVE-2023-6817, CVE-2024-1086

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	2024/03/29	Initial neutralization version
2.2	2024/06/14	CISA note added to bulletin for CVE-2024-1086, TLP changed for CLEAR

Executive summary

The Linux kernel's netfilter component is affected by multiple vulnerabilities which raise significant concern as they could be chained together to achieve significant impact. It is recommended to apply kernel patches as soon as possible.

The uncovering of vulnerabilities within this crucial component, particularly CVE-2023-6817 and CVE-2024-1086, has raised a red flag for security professionals and system administrators.

A severe vulnerability has been discovered in the Linux kernel's nf_tables, known as CVE-2024-1086. This critical flaw allows for local privilege escalation through the improper use of memory. It underscores the necessity of regularly updating the system. CISA added vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation.

An additional security concern of great significance (CVE-2023-6817) has emerged. This particular vulnerability is rooted in a use-after-free error within netfilter's nf_tables component. It is imperative to promptly update the system to mitigate the risk of unauthorized access, emphasizing the importance of timely system updates.

The Linux kernel's netfilter subsystem is at risk due to CVE-2023-3390, a critical loophole that could lead to system crashes and unauthorized code execution. This vulnerability stems from incorrect error handling, resulting in a use-after-free vulnerability.

Vulnerability Info

CVE No.	CVSS Score	Type of Vulnerability
CVE-2023-3390	7.8	CWE-416 Use After Free
CVE-2023-6817	7.8	CWE-416 Use After Free
CVE-2024-1086	7.8	CWE-416 Use After Free

Affected products

All linux kernels may be affected by these vulnerabilities.

In particular RedHat has issued kernel patches for these important vulnerabilities.

Recommendations

Eviden recommends applying the Linux kernel patches as soon as possible.

Available Vendor Patches

For RedHat, see:

1. https://access.redhat.com/security/cve/CVE-2023-3390
2. https://access.redhat.com/security/cve/CVE-2023-6817
3. https://access.redhat.com/security/cve/CVE-2024-1086

Available Workarounds

No workaround is available.

Available Mitigations

Updates for kernel and kernel-rt is now available for Red Hat Enterprise Linux 7, 8 and 9.

Available Exploits/PoC

CVE-2023-3390

Proof of concept is available

https://github.com/google/security-research/blob/master/pocs/linux/kernelctf/CVE-2023-3390_lts_cos_mitigation/docs/exploit.md

CVE-2023-6817

Proof of concept is available

https://seclists.org/oss-sec/2023/q4/316

CVE-2024-1086

Proof of concept is available

https://github.com/Notselwyn/CVE-2024-1086

CISA added vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation.

References

4. https://nvd.nist.gov/vuln/detail/CVE-2023-3390
5. https://nvd.nist.gov/vuln/detail/CVE-2023-6817
6. https://nvd.nist.gov/vuln/detail/CVE-2024-1086
7. http://packetstormsecurity.com/files/174577/Kernel-Live-Patch-Security-Notice-LSN-0097-1.html
8. https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=1240eb93f0616b21c675416516ff3d74798fdc97
9. https://kernel.dance/1240eb93f0616b21c675416516ff3d74798fdc97
10. http://packetstormsecurity.com/files/177029/Kernel-Live-Patch-Security-Notice-LSN-0100-1.html
11. http://www.openwall.com/lists/oss-security/2023/12/22/13
12. http://www.openwall.com/lists/oss-security/2023/12/22/6
13. https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=317eb9685095678f2c9f5a8189de698c5354316a
14. https://kernel.dance/317eb9685095678f2c9f5a8189de698c5354316a
15. https://lists.debian.org/debian-lts-announce/2024/01/msg00005.html
16. https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=f342de4e2f33e0e39165d8639387aa6c19dff660
17. https://github.com/Notselwyn/CVE-2024-1086
18. https://kernel.dance/f342de4e2f33e0e39165d8639387aa6c19dff660
19. https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/7LSPIOMIJYTLZB6QKPQVVAYSUETUWKPF/
20. https://news.ycombinator.com/item?id=39828424
21. https://pwning.tech/nftables/
22. https://access.redhat.com/security/cve/CVE-2023-3390
23. https://access.redhat.com/security/cve/CVE-2023-6817
24. https://access.redhat.com/security/cve/CVE-2024-1086
25. https://www.cisa.gov/news-events/alerts/2024/05/30/cisa-adds-two-known-exploited-vulnerabilities-catalog
26.

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.