EVIDEN
an atos business

Security Bulletin

Red Hat Security Advisories: kernel security update - RHSA-2025_19931

Author(s)	:	Eviden PSIRT
Reference	:	PSIRT-4992
Created	:	18 November 2025
Version	:	2.1
Status	:	Remediation
TLP Classification	:	CLEAR
Document date	:	18 November 2025
Keywords	:	CVE-2022-50367 CVE-2023-53178 CVE-2025-40300

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
2.1	2025/11/18	Initial Eviden version

Executive summary

Red Hat has released a set of security advisories addressing several vulnerabilities in the Linux kernel. The update includes important security fixes designed to protect systems from potential exploits. Users are strongly advised to apply the kernel update promptly to maintain system integrity and prevent unauthorized access.

CVE-2022-50367 – score 7.0

In the Linux kernel, the following vulnerability has been resolved: fs: fix UAF/GPF bug in nilfs_mdt_destroy In alloc_inode, inode_init_always() could return -ENOMEM if security_inode_alloc() fails, which causes inode->i_private uninitialized. Then nilfs_is_metadata_file_inode() returns true and nilfs_free_inode() wrongly calls nilfs_mdt_destroy(), which frees the uninitialized inode->i_private and leads to crashes(e.g., UAF/GPF). Fix this by moving security_inode_alloc just prior to this_cpu_inc(nr_inodes)

CVE-2023-53178 – score 7.3

In the Linux kernel, the following vulnerability has been resolved: mm: fix zswap writeback race condition The zswap writeback mechanism can cause a race condition resulting in memory corruption, where a swapped out page gets swapped in with data that was written to a different page.

CVE-2025-40300 – score. 6.5

In the Linux kernel, the following vulnerability has been resolved: x86/vmscape: Add conditional IBPB mitigation VMSCAPE is a vulnerability that exploits insufficient branch predictor isolation between a guest and a userspace hypervisor (like QEMU). Existing mitigations already protect kernel/KVM from a malicious guest. Userspace can additionally be protected by flushing the branch predictors after a VMexit. Since it is the userspace that consumes the poisoned branch predictors, conditionally issue an IBPB after a VMexit and before returning to userspace. Workloads that frequently switch between hypervisor and userspace will incur the most overhead from the new IBPB. This new IBPB is not integrated with the existing IBPB sites. For instance, a task can use the existing speculation control prctl() to get an IBPB at context switch time. With this implementation, the IBPB is doubled up: one at context switch and another before running userspace. The intent is to integrate and optimize these cases post-embargo. [dhansen: elaborate on suboptimal IBPB solution]

RHSA-2025_19931

RHSA-2025_19931	Red Hat Security Advisory: kernel security update
CVE	CVE-2022-50367 CVE-2023-53178 CVE-2025-40300
Summary	**An update for kernel is now available for Red Hat Enterprise Linux 8.**
Description	Red Hat Product Security has rated this update as having a security impact of Moderate. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section. The kernel packages contain the Linux kernel, the core of any Linux operating system. Security Fix(es): • kernel: x86/vmscape: Add conditional IBPB mitigation (CVE-2025-40300) • kernel: mm: fix zswap writeback race condition (CVE-2023-53178) • kernel: fs: fix UAF/GPF bug in nilfs_mdt_destroy (CVE-2022-50367) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

Affected products

Linux Kernels used in all Eviden products are updated on a regular basis to guarantee that they are not older than 6 month when products are released.

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.

Recommendations

Using uname -r you can check the current running kernel version. The version provided by this patch is kernel-4.18.0-553.83.1.el8_10. Recommendation is to check that running kernel version is at least this level.

Available Vendor Patches

It is highly recommended to apply the latest kernel security patches released by Red Hat without delay. These updates contain critical fixes that address vulnerabilities which could be exploited by attackers. Prompt installation of these patches helps ensure your systems remain secure and stable. Regularly updating your systems with Red Hat's security fixes is essential for maintaining a strong defense against potential threats.

Available Workarounds

No workaround is available.

Available Mitigations

No mitigation identified.

Available Exploits/PoC

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

References

1. https://access.redhat.com/errata/RHSA-2025:19931

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.