EVIDEN
an atos business

Security Bulletin

Red Hat Security Advisories: kernel security update - RHSA-2025_15008

Author(s)	:	**Eviden PSIRT**
Reference	:	**PSIRT-4154**
Created	:	**09 September 2025**
Version	:	**2.2**
Status	:	**Remediation**
TLP Classification	:	**CLEAR**
Document date	:	**3 February 2026**
Keywords	:	**CVE-2025-38211 CVE-2025-38332 CVE-2025-38464 CVE-2025-38477**

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	2025/09/09	Initial Eviden version
2.2	2026/02/03	Remediation 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-2025-38211 - score 7.3

In the Linux kernel, the following vulnerability has been resolved: RDMA/iwcm: Fix use-after-free of work objects after cm_id destruction The commit 59c68ac31e15 ("iw_cm: free cm_id resources on the last deref") simplified cm_id resource management by freeing cm_id once all references to the cm_id were removed.

CVE-2025-38332 - score 7.0

In the Linux kernel, the following vulnerability has been resolved: scsi: lpfc: Use memcpy() for BIOS version The strlcat() with FORTIFY support is triggering a panic because it thinks the target buffer will overflow although the correct target buffer size is passed in. Anyway, instead of memset() with 0 followed by a strlcat(), just use memcpy() and ensure that the resulting buffer is NULL terminated. BIOSVersion is only used for the lpfc_printf_log() which expects a properly terminated string.

CVE-2025-38464 - score 7.3

In the Linux kernel, the following vulnerability has been resolved: tipc: Fix use-after-free in tipc_conn_close(). syzbot reported a null-ptr-deref in tipc_conn_close() during netns dismantle. [0] tipc_topsrv_stop() iterates tipc_net(net)->topsrv->conn_idr and calls tipc_conn_close() for each tipc_conn. The problem is that tipc_conn_close() is called after releasing the IDR lock.

CVE-2025-38477 - score 7.3

In the Linux kernel, the following vulnerability has been resolved: net/sched: sch_qfq: Fix race condition on qfq_aggregate A race condition can occur when

'agg' is modified in qfq_change_agg (called during qfq_enqueue) while other threads access it concurrently. For example, qfq_dump_class may trigger a NULL dereference, and qfq_delete_class may cause a use-after-free. This patch addresses the issue by: 1. Moved qfq_destroy_class into the critical section. 2. Added sch_tree_lock protection to qfq_dump_class and qfq_dump_class_stats.

RHSA-2025_15008

RHSA-2025_15008	Red Hat Security Advisory: kernel security update
CVE	CVE-2025-38211 CVE-2025-38332 CVE-2025-38464 CVE-2025-38477
Summary	**An update for kernel is now available for Red Hat Enterprise Linux 9.**
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: RDMA/iwcm: Fix use-after-free of work objects after cm_id destruction (CVE-2025-38211) • kernel: scsi: lpfc: Use memcpy() for BIOS version (CVE-2025-38332) • kernel: tipc: Fix use-after-free in tipc_conn_close() (CVE-2025-38464) • kernel: net/sched: sch_qfq: Fix race condition on qfq_aggregate (CVE-2025-38477) 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-4.18.0-553.72.1.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-2025:15008

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.