

## Security Bulletin

# Red Hat Security Advisories: kernel security update - RHSA- 2025\_2270

Author(s) : Eviden PSIRT  
Reference : PSIRT-4550  
Created : 26 September 2025  
Version : 0.1  
Status : Neutralization  
TLP Classification : CLEAR  
Document date : 26 September 2025  
Keywords : CVE-2019-25162 CVE-2021-47432 CVE-2023-52648  
CVE-2023-52683 CVE-2023-52791 CVE-2024-26740  
CVE-2024-26759 CVE-2024-26843 CVE-2024-26846  
CVE-2024-26894 CVE-2024-27395 CVE-2024-35947  
CVE-2024-35959 CVE-2024-36905 CVE-2024-39276  
CVE-2024-42292 CVE-2024-43889 CVE-2024-44935  
CVE-2024-44990 CVE-2024-49949 CVE-2024-50099

### **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     | 2025/09/26 | 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-2019-25162](#)

In the Linux kernel, the following vulnerability has been resolved: i2c: Fix a potential use after free Free the adap structure only after we are done using it. This patch just moves the put\_device() down a bit to avoid the use after free. [wsa: added comment to the code, added Fixes tag]

### [CVE-2021-47432](#)

In the Linux kernel, the following vulnerability has been resolved: lib/generic-radix-tree.c: Don't overflow in peek() When we started spreading new inode numbers throughout most of the 64 bit inode space, that triggered some corner case bugs, in particular some integer overflows related to the radix tree code. Oops.

### [CVE-2023-52648](#)

In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: Unmap the surface before resetting it on a plane state Switch to a new plane state requires unreferencing of all held surfaces. In the work required for mob cursors the mapped surfaces started being cached but the variable indicating whether the surface is currently mapped was not being reset. This leads to crashes as the duplicated state, incorrectly, indicates the that surface is mapped even when no surface is present.

### [CVE-2023-52683](#)

In the Linux kernel, the following vulnerability has been resolved: ACPI: LPIT: Avoid u32 multiplication overflow In lpit\_update\_residency() there is a possibility of overflow in multiplication, if tsc\_khz is large enough (> UINT\_MAX/1000). Change

multiplication to `mul_u32_u32()`. Found by Linux Verification Center (linuxtesting.org) with SVACE.

#### [CVE-2023-52791](#)

In the Linux kernel, the following vulnerability has been resolved: i2c: core: Run atomic i2c xfer when !preemptible Since `bae1d3a05a8b`, i2c transfers are non-atomic if preemption is disabled. However, non-atomic i2c transfers require preemption (e.g. in `wait_for_completion()` while waiting for the DMA). `panic()` calls `preempt_disable_notracer()` before calling `emergency_restart()`. Therefore, if an i2c device is used for the restart, the xfer should be atomic. This avoids warnings like: [ 12.667612] WARNING: CPU: 1 PID: 1 at kernel/rcu/tree\_plugin.h:318 rcu\_note\_context\_switch+0x33c/0x6b0 [ 12.676926] Voluntary context switch within RCU read-side critical section! ... [ 12.742376] schedule\_timeout from wait\_for\_completion\_timeout+0x90/0x114 [ 12.749179] wait\_for\_completion\_timeout from tegra\_i2c\_wait\_completion+0x40/0x70 ... [ 12.994527] atomic\_notifier\_call\_chain from machine\_restart+0x34/0x58 [ 13.001050] machine\_restart from panic+0x2a8/0x32c Use !preemptible() instead, which is basically the same check as pre-v5.2.

#### [CVE-2024-26740](#)

In the Linux kernel, the following vulnerability has been resolved: net/sched: act\_mirred: use the backlog for mirrored ingress The test Davide added in commit `ca22da2fbd69` ("act\_mirred: use the backlog for nested calls to mirrored ingress") hangs our testing VMs every 10 or so runs, with the familiar `tcp_v4_rcv -> tcp_v4_rcv` deadlock reported by lockdep. The problem as previously described by Davide (see Link) is that if we reverse flow of traffic with the redirect (egress -> ingress) we may reach the same socket which generated the packet. And we may still be holding its socket lock. The common solution to such deadlocks is to put the packet in the Rx backlog, rather than run the Rx path inline. Do that for all egress -> ingress reversals, not just once we started to nest mirrored calls. In the past there was a concern that the backlog indirection will lead to loss of error reporting / less accurate stats. But the current workaround does not seem to address the issue.

#### [CVE-2024-26759](#)

In the Linux kernel, the following vulnerability has been resolved: mm/swap: fix race when skipping swapcache When skipping swapcache for `SWP_SYNCHRONOUS_IO`, if two or more threads swapin the same entry at the same time, they get different pages (A, B). Before one thread (T0) finishes the swapin and installs page (A) to the PTE, another thread (T1) could finish swapin of page (B), `swap_free` the entry, then swap out the possibly modified page reusing the same entry.

### [CVE-2024-26843](#)

In the Linux kernel, the following vulnerability has been resolved: efi: runtime: Fix potential overflow of soft-reserved region size md\_size will have been narrowed if we have >= 4GB worth of pages in a soft-reserved region.

### [CVE-2024-26846](#)

In the Linux kernel, the following vulnerability has been resolved: nvme-fc: do not wait in vain when unloading module The module exit path has race between deleting all controllers and freeing 'left over IDs'. To prevent double free a synchronization between nvme\_delete\_ctrl and ida\_destroy has been added by the initial commit. There is some logic around trying to prevent from hanging forever in wait\_for\_completion, though it does not handling all cases. E.g. blktests is able to reproduce the situation where the module unload hangs forever. If we completely rely on the cleanup code executed from the nvme\_delete\_ctrl path, all IDs will be freed eventually. This makes calling ida\_destroy unnecessary. We only have to ensure that all nvme\_delete\_ctrl code has been executed before we leave nvme\_fc\_exit\_module. This is done by flushing the nvme\_delete\_wq workqueue. While at it, remove the unused nvme\_fc\_wq workqueue too.

### [CVE-2024-26894](#)

In the Linux kernel, the following vulnerability has been resolved: ACPI: processor\_idle: Fix memory leak in acpi\_processor\_power\_exit() After unregistering the CPU idle device, the memory associated with it is not freed, leading to a memory leak: unreferenced object 0xffff896282f6c000 (size 1024): comm "swapper/0", pid 1, jiffies 4294893170 hex dump (first 32 bytes): 00 00 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... backtrace (crc 8836a742): [<ffffffff993495ed>] kmalloc\_trace+0x29d/0x340 [<ffffffff9972f3b3>] acpi\_processor\_power\_init+0xf3/0x1c0 [<ffffffff9972d263>] \_\_acpi\_processor\_start+0xd3/0xf0 [<ffffffff9972d2bc>] acpi\_processor\_start+0x2c/0x50 [<ffffffff99805872>] really\_probe+0xe2/0x480 [<ffffffff99805c98>] \_\_driver\_probe\_device+0x78/0x160 [<ffffffff99805daf>] driver\_probe\_device+0x1f/0x90 [<ffffffff9980601e>] \_\_driver\_attach+0xce/0x1c0 [<ffffffff99803170>] bus\_for\_each\_dev+0x70/0xc0 [<ffffffff99804822>] bus\_add\_driver+0x112/0x210 [<ffffffff99807245>] driver\_register+0x55/0x100 [<ffffffff9aee4acb>] acpi\_processor\_driver\_init+0x3b/0xc0 [<ffffffff990012d1>] do\_one\_initcall+0x41/0x300 [<ffffffff9ae7c4b0>] kernel\_init\_freeable+0x320/0x470 [<ffffffff99b231f6>] kernel\_init+0x16/0x1b0 [<ffffffff99042e6d>] ret\_from\_fork+0x2d/0x50 Fix this by freeing the CPU idle device after unregistering it.

### [CVE-2024-27395](#)

In the Linux kernel, the following vulnerability has been resolved: net: openvswitch: Fix Use-After-Free in ovs\_ct\_exit Since kfree\_rcu, which is called in the hlist\_for\_each\_entry\_rcu traversal of ovs\_ct\_limit\_exit, is not part of the RCU read critical section, it is possible that the RCU grace period will pass during the traversal and the key will be free. To prevent this, it should be changed to hlist\_for\_each\_entry\_safe.

### [CVE-2024-35947](#)

In the Linux kernel, the following vulnerability has been resolved: dyndbg: fix old BUG\_ON in >control parser Fix a BUG\_ON from 2009. Even if it looks "unreachable" (I didn't really look), lets make sure by removing it, doing pr\_err and return -EINVAL instead.

### [CVE-2024-35959](#)

In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Fix mlx5e\_priv\_init() cleanup flow When mlx5e\_priv\_init() fails, the cleanup flow calls mlx5e\_selq\_cleanup which calls mlx5e\_selq\_apply() that assures that the `priv->state\_lock` is held using lockdep\_is\_held().

### [CVE-2024-36905](#)

In the Linux kernel, the following vulnerability has been resolved: tcp: defer shutdown(SEND\_SHUTDOWN) for TCP\_SYN\_RECV sockets TCP\_SYN\_RECV state is really special, it is only used by cross-syn connections, mostly used by fuzzers. In the following crash [1], syzbot managed to trigger a divide by zero in tcp\_rcv\_space\_adjust() A socket makes the following state transitions, without ever calling tcp\_init\_transfer(), meaning tcp\_init\_buffer\_space() is also not called. TCP\_CLOSE connect() TCP\_SYN\_SENT TCP\_SYN\_RECV shutdown() -> tcp\_shutdown(sk, SEND\_SHUTDOWN) TCP\_FIN\_WAIT1 To fix this issue, change tcp\_shutdown() to not perform a TCP\_SYN\_RECV -> TCP\_FIN\_WAIT1 transition, which makes no sense anyway.

### [CVE-2024-39276](#)

In the Linux kernel, the following vulnerability has been resolved: ext4: fix mb\_cache\_entry's e\_refcnt leak in ext4\_xattr\_block\_cache\_find() Syzbot reports a warning.

### [CVE-2024-42292](#)

In the Linux kernel, the following vulnerability has been resolved: kobject\_uevent: Fix OOB access within zap\_modalias\_env() zap\_modalias\_env() wrongly calculates

size of memory block to move, so will cause OOB memory access issue if variable MODALIAS is not the last one within its @env parameter, fixed by correcting size to memmove.

#### [CVE-2024-43889](#)

In the Linux kernel, the following vulnerability has been resolved: padata: Fix possible divide-by-0 panic in padata\_mt\_helper() We are hit with a not easily reproducible divide-by-0 panic in padata.c at bootup time.

#### [CVE-2024-44935](#)

In the Linux kernel, the following vulnerability has been resolved: sctp: Fix null-ptr-deref in reuseport\_add\_sock(). syzbot reported a null-ptr-deref while accessing sk2->sk\_reuseport\_cb in reuseport\_add\_sock().

#### [CVE-2024-44990](#)

In the Linux kernel, the following vulnerability has been resolved: bonding: fix null pointer deref in bond\_ipsec\_offload\_ok We must check if there is an active slave before dereferencing the pointer.

#### [CVE-2024-49949](#)

In the Linux kernel, the following vulnerability has been resolved: net: avoid potential underflow in qdisc\_pkt\_len\_init() with UFO After commit 7c6d2ecbda83 ("net: be more gentle about silly gso requests coming from user") virtio\_net\_hdr\_to\_skb() had sanity check to detect malicious attempts from user space to cook a bad GSO packet. Then commit cf9acc90c80ec ("net: virtio\_net\_hdr\_to\_skb: count transport header in UFO") while fixing one issue, allowed user space to cook a GSO packet.

#### [CVE-2024-50099](#)

In the Linux kernel, the following vulnerability has been resolved: arm64: probes: Remove broken LDR (literal) uprobe support The simulate\_ldr\_literal() and simulate\_ldrsw\_literal() functions are unsafe to use for uprobes. Both functions were originally written for use with kprobes, and access memory with plain C accesses. When uprobes was added, these were reused unmodified even though they cannot safely access user memory.

### **RHSA-2025\_2270**

|                |                                                                   |
|----------------|-------------------------------------------------------------------|
| RHSA-2025_2270 | <a href="#">Red Hat Security Advisory: kernel security update</a> |
|----------------|-------------------------------------------------------------------|

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE         | <a href="#">CVE-2019-25162</a><br><a href="#">CVE-2021-47432</a><br><a href="#">CVE-2023-52648</a><br><a href="#">CVE-2023-52683</a><br><a href="#">CVE-2023-52791</a><br><a href="#">CVE-2024-26740</a><br><a href="#">CVE-2024-26759</a><br><a href="#">CVE-2024-26843</a><br><a href="#">CVE-2024-26846</a><br><a href="#">CVE-2024-26894</a><br><a href="#">CVE-2024-27395</a><br><a href="#">CVE-2024-35947</a><br><a href="#">CVE-2024-35959</a><br><a href="#">CVE-2024-36905</a><br><a href="#">CVE-2024-39276</a><br><a href="#">CVE-2024-42292</a><br><a href="#">CVE-2024-43889</a><br><a href="#">CVE-2024-44935</a><br><a href="#">CVE-2024-44990</a><br><a href="#">CVE-2024-49949</a><br><a href="#">CVE-2024-50099</a>                                                                                                                              |
| Summary     | <b>An update for kernel is now available for Red Hat Enterprise Linux 9.</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Description | <p>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):</p> <ul style="list-style-type: none"><li>• kernel: use after free in i2c (CVE-2019-25162)</li><li>• kernel: mm/swap: fix race when skipping swapcache (CVE-2024-26759)</li><li>• kernel: net/sched: act_mirred: use the backlog for mirrored ingress (CVE-2024-26740)</li><li>• kernel: nvme-fc: do not wait in vain when unloading module (CVE-2024-26846)</li><li>• kernel: efi: runtime: Fix potential overflow of soft-reserved region size (CVE-2024-26843)</li></ul> |

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <ul style="list-style-type: none"><li>• kernel: ACPI: processor_idle: Fix memory leak in acpi_processor_power_exit() (CVE-2024-26894)</li><li>• kernel: drm/vmwgfx: Unmap the surface before resetting it on a plane state (CVE-2023-52648)</li><li>• kernel: net: openvswitch: Fix Use-After-Free in ovs_ct_exit (CVE-2024-27395)</li><li>• kernel: ACPI: LPIT: Avoid u32 multiplication overflow (CVE-2023-52683)</li><li>• kernel: dyndbg: fix old BUG_ON in</li></ul> |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 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-5.14.0-427.57.1.el9\_4. 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-2025:2270>

## 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. <a href="https://www.first.org/tlp/">https://www.first.org/tlp/</a>       |
| 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<sup>1</sup>

[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.

---

<sup>1</sup> Eviden business is operated through the following brands: AppCentrica, ATHEA, BullSequana, Cloudamize, Cloudreach, Cryptovision, DataSantics, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, IDnomic, In Fidem, Ipsotek, Maven Wave, Profit4SF, SEC Consult, Trustway, Visual BI, Worldgrid, X-Perion.  
Eviden is a registered trademark. © Eviden SAS, 2025.