Overall Rating - High

BRITISH
COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Red Hat published security advisories to address vulnerabilities in multiple products. Included were updates to address vulnerabilities in the Linux kernel for the following products:

- Red Hat CodeReady Linux Builder – multiple versions and platforms
- Red Hat Enterprise Linux – multiple versions and platforms
- Red Hat Enterprise Linux Server – multiple versions and platforms

Technical Details

The kernel-rt packages provide the Real Time Linux Kernel, which enables fine-tuning for systems with extremely high determinism requirements.
Security Fix(es):
- kernel: untrusted VMM can trigger int80 syscall handling (CVE-2024-25744)
- kernel: netfilter: nftables: exthdr: fix 4-byte stack OOB write (CVE-2023-52628)
Bug Fix(es):
- kernel-rt: kernel: untrusted VMM can trigger int80 syscall handling (JIRA:RHEL-30421)
- kernel-rt: kernel: netfilter: nftables: exthdr: fix 4-byte stack OOB write (JIRA:RHEL-31093)
- kernel-rt: update RT source tree to the latest RHEL-9.2 ad hoc schedule build (JIRA:RHEL-34746)

These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify [VRM](#) with any questions or concerns you may have.

References

- CVE-2023-52628 CVE-2023-6717 CVE-2024-1132 CVE-2024-1249 CVE-2024-22259
- [RHSA-2024:2845 - Security Advisory](#)
- [RHSA-2024:2846 - Security Advisory](#)
- [Red Hat Security Advisories](#)