June 19, 2024

Overall Rating: High

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a 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 Enterprise Linux Server – multiple versions and platforms
- Red Hat Enterprise Linux – multiple versions and platforms
- Red Hat CodeReady Linux Builder – multiple versions and platforms
- Red Hat Enterprise Linux for Real Time – multiple versions and platforms

Technical Details

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fix(es):

- kernel: KVM: SEV-ES / SEV-SNP VMGEXIT double fetch vulnerability (CVE-2023-4155)
- kernel: bluetooth: bt_sock_ioctl race condition leads to use-after-free in bt_sock_recvmsg (CVE-2023-51779)
- kernel: wifi: mac80211: fix potential key use-after-free (CVE-2023-52530)

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have
VulnerabilityandRiskManagement@gov.bc.ca

References

- Red Hat Security Advisory - RHSA-2024:3859
- Red Hat Security Advisory - RHSA-2024:3855
- Red Hat Security Advisory - RHSA-2024:3854
- Red Hat Security Advisories
- VRM Vulnerability Reports