

Overall Rating: Critical



This is a technical bulletin intended for technical audiences.

Summary

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

Technical Details

An update for kernel is now available for Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support, Red Hat Enterprise Linux 8.6 Update Services for SAP Solutions, and Red Hat Enterprise Linux 8.6 Telecommunications Update Service.

This vulnerability is rated as a **CRITICAL** risk. Software updates exist to address these risks.

Action Required

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

Please notify [VRM](mailto:vulnerabilityandriskmanagement@gov.bc.ca) with any questions or concerns you may have at vulnerabilityandriskmanagement@gov.bc.ca

References

- CCVE-2021-47548 CVE-2022-48743 CVE-2023-52667 CVE-2023-52784 CVE-2024-26733 CVE-2024-26852 CVE-2024-26908 CVE-2024-35960 CVE-2024-36020 CVE-2024-36025 CVE-2024-36924 CVE-2024-36929 CVE-2024-38596 CVE-2023-6597 CVE-2024-6601 CVE-2024-6602 CVE-2024-6603 CVE-2024-6604
- [Red Hat Security Advisories](#)