July 17, 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 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 Enterprise Linux for Real Time – multiple versions and platforms

Technical Details

A flaw was found in the smb client in the Linux kernel. A potential out-of-bounds error was seen in the smb2_parse_contexts() function. Validate offsets and lengths before dereferencing create contexts in smb2_parse_contexts().

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 at vulnerabilityandriskmanagement@gov.bc.ca

References

- CVE-2023-52434 CVE-2024-0193 CVE-2024-26673
- Red Hat security advisory – RHSA-2024:4412
- Red Hat security advisory – RHSA-2024:4415
- Red Hat security advisory – RHSA-2024:4447
- Red Hat Security Advisories