March 26, 2024

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 for Real Time/for NFV – Telecommunications Update Service 8.4 x86_64
- Red Hat Enterprise Linux Server – multiple versions and platforms

Technical Details

Squid is a web proxy cache. Starting in version 3.5.27 and prior to version 6.8, Squid may be vulnerable to a Denial-of-Service attack against HTTP Chunked decoder due to an uncontrolled recursion bug. This problem allows a remote attacker to cause Denial of Service when sending a crafted, chunked, encoded HTTP Message. This bug is fixed in Squid version 6.8. In addition, patches addressing this problem for the stable releases can be found in Squid's patch archives. There is no workaround for this issue.

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-2024-25111 CVE-2024-25710 CVE-2024-26308 CVE-2023-46809 CVE-2024-21892 CVE-2024-22019 CVE-2024-1394
- Red Hat Security Advisories