October 5, 2023

Overall Rating - High

BRITISH COLUMBIA

Summary

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

- Red Hat Enterprise Linux Server – versions AUS 7.6 x86_64 and AUS 7.7 x86_64

Technical Details

Linux Kernel nftables Out-Of-Bounds Read/Write Vulnerability; nft_byteorder poorly handled vm register contents when CAP_NET_ADMIN is in any user or network namespace.

This vulnerability is rated as a **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-2023-35001, CVE-2023-20593, CVE-2023-32233
- Red Hat Security Advisory – RHSA-2023:5414
- Red Hat Security Advisory – RHSA-2023:5419

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: Cybersecurity Alerts