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 an update for kernel is now available for Red Hat Enterprise Linux 8.

Technical Details

Security Fixes:

- **kernel:** bluetooth: Unauthorized management command execution BZ - 2187308 – CVE-2023-2002
- **kernel:** UAF in nftables when nft_set_lookup_global triggered after handling named and anonymous sets in batch requests BZ - 2213260 - CVE-2023-3390
- **kernel:** cls_flower: out-of-bounds write in fl_set_geneve_opt() BZ - 2215768 - CVE-2023-35788
- **hw:** amd: Cross-Process Information Leak BZ - 2217845 - CVE-2023-20593
- **kernel:** ipvlan: out-of-bounds write caused by unclear skb->cb BZ - 2218672 - CVE-2023-3090
- **kernel:** nf_tables: stack-out-of-bounds-read in of failure in tcf_change_indev function BZ - 2220892 - CVE-2023-35001
- **kernel:** net/sched: cls_fw component can be exploited as result BZ - 2225097 - CVE-2023-3776
- **kernel:** netfilter: use-after-free due to improper element removal in nft_pipapo_remove() BZ - 2225275 - CVE-2023-4004

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

- Red Hat Security Advisory – RHSA-2023:5244
- Red Hat Security Advisories