September 14, 2023

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 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 for x86_64
- Red Hat Enterprise Linux for Real Time for NFV 9 x86_64

Technical Details

Security Fixes:

- BZ - 2181891 - CVE-2023-1637 kernel: save/restore speculative MSRs during S3 suspend/resume
- BZ - 2213260 - CVE-2023-3390 kernel: UAF in nftables when nft_set_lookup_global triggered after handling named and anonymous sets in batch requests
- BZ - 2213455 - CVE-2023-21102 kernel: bypass of shadow stack protection due to a logic error
- BZ - 2217845 - CVE-2023-20593 hw: amd: Cross-Process Information Leak
- BZ - 2220892 - CVE-2023-35001 kernel: nf_tables: stack-out-of-bounds-read in nft_byteorder_eval()
- BZ - 2220893 - CVE-2023-31248 kernel: nf_tables: use-after-free in nft_chain_lookup_byid()
- BZ - 2225097 - CVE-2023-3776 kernel: net/sched: cls_fw component can be exploited as result of failure in tcf_change_indev function
- BZ - 2225198 - CVE-2023-3610 kernel: netfilter: nf_tables: fix chain binding transaction logic in the abort path of NFT_MSG_NEWRULE
- BZ - 2225239 - CVE-2023-4147 kernel: netfilter: nf_tables_newrule when adding a rule with NFTA_RULE_CHAIN_ID leads to use-after-free
- BZ - 2225275 - CVE-2023-4004 kernel: netfilter: use-after-free due to improper element removal in nft_pipapo_remove()

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-2023-1637, CVE-2023-3390, CVE-2023-21102, CVE-2023-20593, CVE-2023-35001, CVE-2023-31248, CVE-2023-3776, CVE-2023-3610, CVE-2023-4147, CVE-2023-4004
- Red Hat Security Advisory – RHSA-2023:5091
- Red Hat Security Advisories

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