May 9, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware Ubuntu published a security notice to address vulnerabilities in the Linux kernel affecting the following products:

- Ubuntu 18.04 ESM
- Ubuntu 20.04 LTS
- Ubuntu 22.04 LTS

Technical Details

In the Linux kernel, the following vulnerability has been resolved: can: j1939: prevent deadlock by changing j1939_socks_lock to rwlock The following 3 locks would race against each other, causing the deadlock situation in the Syzbot bug report: - j1939_socks_lock - active_session_list_lock - sk_session_queue_lock A reasonable fix is to change j1939_socks_lock to an rwlock, since in the rare situations where a write lock is required for the linked list that j1939_socks_lock is protecting, the code does not attempt to acquire any more locks. This would break the circular lock dependency, where, for example, the current thread already locks j1939_socks_lock and attempts to acquire sk_session_queue_lock, and at the same time, another thread attempts to acquire j1939_socks_lock while holding sk_session_queue_lock. NOTE: This patch along does not fix the unregister_netdevice bug reported by Syzbot; instead, it solves a deadlock situation to prepare for one or more further patches to actually fix the Syzbot bug, which appears to be a reference counting problem within the j1939 codebase. [mkl: remove unrelated newline change]

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

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.

References

- CVE-2024-34397 CVE-2023-52604 CVE-2023-52597 CVE-2024-26636 CVE-2024-26645 CVE-2024-26600 CVE-2023-52638 CVE-2023-52622 CVE-2023-52491 CVE-2023-52602 CVE-2023-51792 CVE-2024-28182 CVE-2024-4418 CVE-2024-3096 CVE-2024-2756 CVE-2022-4900 CVE-2024-2961
- Ubuntu Security Notice - LSN-0103-1
- Ubuntu Security Notices