July 8, 2024

Overall Rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a recently released Ubuntu Security Bulletin. The vulnerabilities in the Linux kernel affecting the following products:

- Ubuntu 16.04 ESM
- Ubuntu 18.04 ESM
- Ubuntu 20.04 LTS
- Ubuntu 22.04 LTS
- Ubuntu 23.10
- Ubuntu 24.04 LTS

Technical Details

The Apache HTTP Server mod rewrite module incorrectly handled certain substitutions. A remote attacker could possibly use this issue to execute scripts in directories not directly reachable by any URL, or cause a denial of service. Some environments may require using the new UnsafeAllow3F flag to handle unsafe substitutions.
(CVE-2024-38474, CVE-2024-38475, CVE-2024-39573)

This vulnerability is rated as a **CRITICAL** risk. Software updates exist 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
vulnerabilityandriskmanagement@gov.bc.ca

References

- CVE-2024-39473 CVE-2024-38474 CVE-2024-38475 CVE-2024-32498 CVE-2023-48945 CVE-2023-31631 CVE-2023-48951 CVE-2021-33631 CVE-2021-47063 CVE-2023-52615 CVE-2024-21823 CVE-2024-26924 CVE-2024-26643 CVE-2024-26924 CVE-2024-26643 CVE-2024-26925 CVE-2024-21823 CVE-2024-21824 CVE-2024-26643
- Ubuntu Security Notices