December 1, 2023

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 numerous Ubuntu vulnerabilities. The vulnerabilities affect Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, Ubuntu 23.04 and Ubuntu 23.10.

Technical Details

Ubuntu has identified ten CVEs that should be considered as HIGH priorities to patch – CVE-2023-4623 A use-after-free vulnerability in the Linux kernel's can be exploited to achieve local privilege escalation. CVE-2023-42752 An integer overflow flaw was found in the Linux kernel. CVE-2023-42753 An array indexing vulnerability was found in the netfilter subsystem of the Linux kernel. CVE-2023-40283 An issue was discovered in the Linux kernel before 6.4.10. CVE-2023-4004 A use-after-free flaw was found in the Linux kernel's netfilter. This issue could allow a local user to crash the system or potentially escalate their privileges on the system. CVE-2023-3776 A use-after-free vulnerability in the Linux kernel can be exploited to achieve local privilege escalation. CVE-2023-3777 A use-after-free vulnerability in the Linux kernel's netfilter component can be exploited to achieve local privilege escalation. CVE-2023-3609 A use-after-free vulnerability in the Linux kernel component can be exploited to achieve local privilege escalation. CVE-2023-3567 A use-after-free flaw was found in the Linux Kernel. CVE-2023-31436 in the Linux kernel before 6.2.13 allows an out-of-bounds write.

Additionally, there are nine critical vulnerabilities (CVSS of 9.1 to 9.8) CVE-2023-45871, CVE-2023-39352, CVE-2023-36328, CVE-2023-25775, CVE-2022-48522, CVE-2022-37454, CVE-2023-39356, CVE-2023-38432, CVE-2023-38430 that also should be considered high priorities.

As there are numerous vulnerabilities, detailed in the Ubuntu references below, VRM recommends reviewing the notifications and CVEs detailing the vulnerabilities, mitigations and links to updates for your organizational systems.

Select the Ubuntu version in the reference section below to access all vulnerabilities and security fixes available for that Ubuntu version.

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

- Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, Ubuntu 23.04 , Ubuntu 23.10
- Ubuntu Security Notices
- VRM Vulnerability Reports
- CVE-2023-6212, CVE-2023-6209, CVE-2023-6208, CVE-2023-6207, CVE-2023-6206, CVE-2023-6205, CVE-2023-6204, CVE-2023-5717, CVE-2023-5366, CVE-2023-5345, CVE-2023-5197, CVE-2023-5090, CVE-2023-4881, CVE-2023-47038, CVE-2023-4623, CVE-2023-4622, CVE-2023-45871, CVE-2023-45862, CVE-2023-44446, CVE-2023-44444, CVE-2023-44443, CVE-2023-44442, CVE-2023-44441, CVE-2023-44429, CVE-2023-42754, CVE-2023-42753, CVE-2023-42752, CVE-

2023-4134, CVE-2023-4132, CVE-2023-40476, CVE-2023-40475, CVE-2023-40474, CVE-2023-40283, CVE-2023-40217, CVE-2023-4004, CVE-2023-3995, CVE-2023-39356, CVE-2023-39352, CVE-2023-39194, CVE-2023-39193, CVE-2023-39192, CVE-2023-39189, CVE-2023-3867, CVE-2023-3866, CVE-2023-3865, CVE-2023-3863, CVE-2023-38432, CVE-2023-38430, CVE-2023-3777, CVE-2023-3776, CVE-2023-3772, CVE-2023-37329, CVE-2023-36328, CVE-2023-3609, CVE-2023-3567, CVE-2023-34319, CVE-2023-31436, CVE-2023-31085, CVE-2023-31083, CVE-2023-25775, CVE-2023-22081, CVE-2023-22067, CVE-2023-22025, CVE-2022-48564, CVE-2022-48522, CVE-2022-41877, CVE-2022-40433, CVE-2022-37454, CVE-2022-3643, CVE-2022-32990, CVE-2022-30790, CVE-2022-30552, CVE-2022-30067, CVE-2022-2347, CVE-2018-8050,