Security Advisory 2023-054

Privilege Escalation Vulnerabilities in Ubuntu

July 27, 2023 — v1.0

TLP:CLEAR

History:

- *27/07/2023 — v1.0 – Initial publication*

Summary

On the 24th of July, 2023, Ubuntu issued a fix for two local privilege escalation vulnerabilities, **CVE-2023-2640** and **CVE-2023-32629**, that were discovered in the OverlayFS module of its Linux kernel [1].

CVE-2023-2640 is due to permission check and has a CVSS score of 7.8 out of 10.

CVE-2023-32629 is due to permission check and has a CVSS score of 7.8 out of 10.

Technical Details

The two vulnerabilities are exclusive to Ubuntu because of the changes Ubuntu introduced in the OverlayFS module in 2018. These modifications did not pose any risks initially. However, they later led to an unpatched vulnerable flow in Ubuntu after the discovery and fixing of a security vulnerability in the Linux kernel in 2020 [1].

Affected Products

Based on the research [1], the following Ubuntu releases and versions are impacted:

- Ubuntu 23.04 (Lunar Lobster) Version 6.2.0
- Ubuntu 22.10 (Kinetic Kudu) Version 5.19.0
- Ubuntu 22.04 LTS (Jammy Jellyfish) Versions 5.19.0 and 6.2.0
- Ubuntu 20.04 LTS (Focal Fossa) Version 5.4.0 (Only affected by CVE-2023-32629)
- Ubuntu 18.04 LTS (Bionic Beaver) Version 5.4.0 (Only affected by CVE-2023-32629)

This information is still being updated as more data becomes available from the official security bulletins for both CVEs [2][3].

Recommendations

CERT-EU recommends reviewing Ubuntu's security bulletins [2][3] and applying the necessary updates.

References

[1] https://www.wiz.io/blog/ubuntu-overlayfs-vulnerability

[2] https://ubuntu.com/security/CVE-2023-32629

[3] https://ubuntu.com/security/CVE-2023-2640