AL2024_02 New critical Linux vulnerability affects major distributions. (February 6, 2024)

Description

Recently, an alarming security vulnerability was discovered in the widely used GNU C library (glibc), which exists in most major Linux versions. This flaw allows for the possibility of local privilege escalation (LPE), which is potentially catastrophic for users.

Details

Being tracked as CVE-2023-6246, this vulnerability is found in the GNU C library, specifically in the glibc's vsyslog_internal() function that is used in the widely popular syslog and vsyslog protocols. The syslog and vsyslog protocols are used by computer systems to send event data logs to a central location for storage. This vulnerability is caused by a heap-based buffer overflow that was accidentally introduced in glibc version 2.37. The buffer overflow requires specific conditions to be exploited (i.e. an unusually long argv[0] or openlog() ident argument) that if successful, can grant an unprivileged user full root access to the system.

Researchers at Quals have tested and confirmed that Debian 12 and 13, Ubuntu 23.04 and 23.10, and Fedora 37 to 39 were all vulnerable to this exploit. It should be noted that other Linux distributions not tested may be exploitable.

Remediation

It is highly recommended to update the glibc library to the latest version, 2.39. The glibc version can be verified by running this command in the terminal, "$ ldd --version". Furthermore, it is recommended to update all Linux distributions in use to their latest versions.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Gatlan, S. (2024, January 30). *New Linux glibc flaw lets attackers get root on major distros.* BleepingComputer. https://www.bleepingcomputer.com/news/security/new-linux-glibc-flaw-lets-attackers-get-root-on-major-distros/

- Abbasi, S. (2024, February 1). *Qualys TRU Discovers Important Vulnerabilities in GNU C Library's syslog() | Qualys Security Blog.* Qualys Security Blog. https://blog.qualys.com/vulnerabilities-threat-research/2024/01/30/qualys-tru-discovers-important-vulnerabilities-in-gnu-c-librarys-syslog