Security Advisory 2023-072

GNU C Library Dynamic Loader Buffer Overflow Vulnerability

October 4, 2023 — v1.0

TLP:CLEAR

History:

- *4/10/2023 — v1.0 – Initial publication*

Summary

A critical buffer overflow vulnerability, identified as `CVE-2023-4911`, has been discovered by Qualys Research Labs in the GNU C Library's dynamic loader when processing the `GLIBC_TUNABLES` environment variable. This vulnerability can be exploited to obtain full root privileges, impacting several major Linux distributions.

It is recommended updating as soon as possible.

Technical Details

The GNU C Library's dynamic loader is responsible for locating and loading shared libraries needed by a program. It operates with elevated privileges when executing a set-user-ID program, set-group-ID program, or a program with capabilities.

The vulnerability `CVE-2023-4911` specifically relates to the processing of the `GLIBC_TUNABLES` environment variable. It was introduced in glibc 2.34 in April 2021 by the commit `2ed18c`. When ld.so starts its execution, it invokes `__tunables_init()` to search for `GLIBC_TUNABLES` variables. Upon finding any, it makes a copy and proceeds to sanitise this copy. However, due to incorrect handling, a buffer overflow can be triggered and leveraged to obtain full root privileges.

Affected Products

The following distributions before the patch and in their default installation were successfully exploited by Qualys' team:

- Fedora 37 and 38
- Ubuntu 22.04 and 23.04
- Debian 12 and 13

Other distributions might be vulnerable except for Alpine Linux which utilises musl libc instead of glibc.

Recommendations

Users and administrators are urged to apply patches as soon as they are available from their respective distribution's repository.

References

[1] https://www.qualys.com/2023/10/03/cve-2023-4911/looney-tunables-local-privilege-escalation-glibc-ld-so.txt

[2] https://www.debian.org/security/2023/dsa-5514