CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-040

Privilege Escalation Vulnerability in Linux Kernel

July 22, 2021 — v1.0

TLP:WHITE

History:

- *22/07/2021 — v1.0 – Initial publication*

Summary

A vulnerability (CVE-2021-33909) in the Linux kernel filesystem layer may allow local, unprivileged user to gain root privileges on a vulnerable host by exploiting this vulnerability in a default configuration. The vulnerability is dubbed *Sequoia* [1].

Technical Details

`fs/seq_file.c` file in the affected Linux kernels does not properly restrict seqential buffer allocations, leading to an integer overflow, an out-of-bounds write, and escalation to root by an unprivileged user. Virtual file system implementation in the Linux kernel contained an unsigned to signed integer conversion error. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code.

Affected Products

Linux distros using kernel 3.16 through 5.13.x before 5.13.4

Recommendations

Follow the instructions from the specific distro to update. For the most common you can reffer to [2, 3, 4].

CERT-EU recommends updating the vulnerable systems as soon as possible.

Workaround

Qualys, who discoverd this bug, has created an exploit as a PoC as well as mitigations to prevent their specific exploit from working [1]. Other exploitation techniques may exist. To completely fix this vulnerability, the kernel must be patched.

References

[1] https://blog.qualys.com/vulnerabilities-threat-research/2021/07/20/sequoia-a-local-privilege-escalation-vulnerability-in-linuxs-filesystem-layer-cve-2021-33909

[2] https://ubuntu.com/security/CVE-2021-33909

[3] https://security-tracker.debian.org/tracker/CVE-2021-33909

[4] https://access.redhat.com/security/cve/cve-2021-33909