CERT-EU

Security Advisory 2022-018

Serious Vulnerability in Linux Kernel

March 17, 2022 — v1.0

TLP:WHITE

History:

- *17/03/2022 — v1.0 – Initial publication*

Summary

On February 22, Red Hat released a security advisory for fixing a severe vulnerability in the `netfilter` subcomponent in the Linux kernel. Listed as CVE-2022-25636 with a CVSS score of 7.8, it could allow a local attacker with a user account on the system to gain access to out-of-bounds memory, leading to a system crash or a privilege escalation [1]. This vulnerability is present in all recent major distributions and **exploits for this vulnerability ware already published** [2].

It is recommended to update the Linux distributions as soon as possible.

Technical Details

An out-of-bounds (OOB) memory access flaw was found in `nft_fwd_dup_netdev_offload` in `net/netfilter/nf_dup_netdev.c` in the `netfilter` subcomponent in the Linux kernel due to a heap out-of-bounds write problem [2].

Affected Products

This vulnerability is present in the Linux kernel versions 5.4 through 5.6.10. on all major distributions such as Red Hat Enterprise Linux (RHEL) 8.x; Debian Bullseye; Ubuntu Linux, and SUSE Linux Enterprise 15.3 [3].

While the Linux kernel `netfilter` patch has been made available [4], the patch is not available yet in all distributions.

Recommendations and Mitigations

CERT-EU recommends following the specific steps listed for each of the following Linux distributions:

- Debian Bullseye, more details in [5];
- Ubuntu releases, more details in [6];
- Suse Linux Enterprise, more details in [7] and [8];
- RedHat Hat Enterprise Linux more details in [9].

References

[1] https://access.redhat.com/security/cve/CVE-2022-25636

[2] https://nickgregory.me/linux/security/2022/03/12/cve-2022-25636/

[3] https://www.zdnet.com/article/nasty-linux-netfilter-firewall-security-hole-found/

[4] https://git.kernel.org/pub/scm/linux/kernel/git/netfilter/nf.git/commit/?id=b1a5983f56e371046dcf164f90bfaf704

[5] https://security-tracker.debian.org/tracker/CVE-2022-25636

[6] https://ubuntu.com/security/CVE-2022-25636

[7] https://www.suse.com/security/cve/CVE-2022-25636.html

[8] https://www.suse.com/support/kb/doc/?id=000020615

[9] https://access.redhat.com/security/cve/CVE-2022-25636