Hive Pro

THREAT ADVISORY

Attackers could gain root access using vulnerability in Linux Kernel Netfilter Firewall

TA2022063

Threat Level **AMBER**

Publish Date – March 17, 2022

A flaw in the Linux kernel has been discovered. If exploited, this flaw could allow a local attacker to gain privileges on targeted systems, allowing them to escape containers, execute arbitrary code, or cause a kernel panic.

This heap out-of-bounds write vulnerability has been assigned CVE-2022-25636 and affects the Linux kernel's netfilter subcomponent. Netfilter is a Linux kernel framework that enables various networking-related operations such as packet filtering, network address translation, and port translation. The bug is related to an issue with the framework's incorrect handling of the hardware offload feature, which could be utilized by a local attacker to cause a denial-of-service (DoS) or possibly execute arbitrary code.

This issue has been fixed in Linux kernel version 5.7 and vendors such as RedHat, SUSE, Ubuntu, and Oracle has also made a fix available for the same.

Potential MITRE ATT&CK TTPs are:
TA0042: Resource Development
T1588: Obtain Capabilities
T1588.006: Obtain Capabilities: Vulnerabilities
TA0001: Initial Access
T1190: Exploit Public-Facing Application
TA0040: Impact
T1499: Endpoint Denial of Service
T1499.004: Endpoint Denial of Service: Application or System Exploitation

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-25636	Linux kernel versions 5.4 to 5.6.10	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	kernel: heap out of bounds write in nf_dup_netdev.c	CWE-787

Patch Link

https://git.kernel.org/pub/scm/linux/kernel/git/netfilter/nf.git/snapshot/nf-b1a5983f56e371046dcf164f90bfaf704d2b89f6.tar.gz

References

https://nickgregory.me/linux/security/2022/03/12/cve-2022-25636/
https://access.redhat.com/security/cve/CVE-2022-25636
https://www.openwall.com/lists/oss-security/2022/02/21/2
https://security-tracker.debian.org/tracker/CVE-2022-25636
https://linux.oracle.com/cve/CVE-2022-25636.html
https://www.suse.com/security/cve/CVE-2022-25636.html
https://ubuntu.com/security/CVE-2022-25636