مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Linux Kernel Privilege Escalation Vulnerability

Tracking #:432315908

Date:31-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a Linux Kernel Privilege Escalation Vulnerability is is actively exploited by threat actors.

TECHNICAL DETAILS:

A privilege escalation vulnerability (**CVE-2024-1086)** has been identified in the Linux kernel's netfilter: nf_tables component. This vulnerability allows an attacker with unprivileged access to potentially gain full root privileges on a vulnerable system. This significantly elevates the attacker's capabilities and could lead to complete system compromise. A proof-of-concept (PoC) tool have been publicly disclosed recently an is added to Known Exploited Vulnerabilities Catalog.

Affected Versions:

- Affected Versions: 3.15 <= Linux kernel <= 6.8-rc1
- Known distributions such as Redhat, Ubuntu, Debian, etc., are affected.

Unaffected Versions:

- Linux kernel >= 6.8-rc2

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions for Linux Kernel.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

https://nvd.nist.gov/vuln/detail/CVE-2024-1086