مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Vulnerability in Linux Kernel

Tracking #:432317146

Date:29-04-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a security flaw in the Linux kernel that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-21756**
- A critical Use-After-Free (UAF) vulnerability exists in the Linux kernel's vsock subsystem. This vulnerability arises from improper handling of socket binding states during transport reassignment, leading to the premature freeing of vsock objects.
- Successful exploitation allows attackers to bypass Kernel Address Space Layout Randomization (kASLR), escalate privileges, and execute code in the kernel.
- A proof-of-concept (PoC) for CVE-2025-21756 is publicly available, increasing the risk of exploitation.

Affected Components:

- Linux Kernel vsock subsystem

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Linux distribution vendor.

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-2025-21756
- https://hoefler.dev/articles/vsock.html
- https://github.com/hoefler02/CVE-2025-21756