مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Actively Exploited Vulnerability in Linux Kernel

Tracking #:432317389
Date:18-06-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical privilege escalation vulnerability in the Linux kernel's OverlayFS subsystem, tracked as CVE-2023-0386, is being actively exploited in the wild.

TECHNICAL DETAILS:

A critical privilege escalation vulnerability in the Linux kernel's OverlayFS subsystem, tracked as CVE-2023-0386, is being actively exploited in the wild. The vulnerability arises from improper handling of setuid/setgid bits during file copy-up operations between mounts. As a result, an unprivileged local user can craft an exploit to gain root-level access in seconds.

A publicly available proof-of-concept demonstrates reliable exploitation on systems such as Ubuntu 22.04, making this threat particularly severe for environments where OverlayFS, user namespaces, or container technologies are in use. The flaw enables attackers to bypass privilege boundaries in shared hosting, desktop Linux, CI pipelines, and containerized deployments.

Immediate remediation is urged to prevent unauthorized root access on affected systems

Vulnerability Details:

- CVE ID: CVE-2023-0386- Linux Kernel Improper Ownership Management Vulnerability
- Vulnerability Type: Local Privilege Escalation
- Attack Vector: Local (via unprivileged user)
- CVSS v3.1 Score: 7.8 (High)
- Affected Component: OverlayFS in Linux Kernel
- Exploit Code: Public and verified working. The PoC was tested on Ubuntu 22.04 and successfully elevated a non-privileged user to full root access.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade to a patched version of the Linux kernel Immediately.

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://www.cve.org/CVERecord?id=CVE-2023-0386