

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Multiple Vulnerabilities in Linux Kernel
Tracking #:432315747
Date:03-04-2024

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 INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities have been identified in the Linux Kernel which could allow an unprivileged attacker to execute a DoS attack on a targeted system.

TECHNICAL DETAILS:

- **CVE-2024-26653:** This vulnerability resides in the ljca driver and is classified as a double free issue. Exploiting this vulnerability could lead to system crashes.
- **CVE-2024-26654:** This vulnerability affects the ALSA (Advanced Linux Sound Architecture) subsystem and is classified as a Use-After-Free (UAF) bug. A successful exploit could result in system crashes or potential privilege escalation.

Affected Product:

- Linux Kernel v2.6.23, v6.7.0

Fixed Versions:

- Linux Kernel v6.9-rc2

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to apply the latest security patches from Linux distribution provider as soon as possible

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:

1. <https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/>