مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical eBPF Vulnerabilities in Linux Kernel

Tracking #:432316808

Date:30-01-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed high-severity vulnerabilities in the Linux kernel's eBPF framework, which could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

High-Severity vulnerabilities, CVE-2024-56614 and CVE-2024-56615, exists in the Linux kernel's eBPF framework, specifically affecting its AF_XDP sockets for high-performance packet processing. Both vulnerabilities have a CVSS score of 7.8, indicating their potential for serious security risks.

Vulnerability Details:

- **CVE-2024-56614**: Affects the xsk_map_delete_elem function in AF_XDP sockets.
- **CVE-2024-56615**: Impacts the devmap_map_delete_elem function associated with DEVMAP.
- CVSS score 7.8 High
- Both vulnerabilities stem from integer overflow errors that can lead to out-of-bounds writes and memory corruption. The root cause is an implicit type conversion between unsigned and signed integers during bounds checks, allowing negative values to bypass checks and potentially result in memory corruption and control flow hijacking.
- Successful exploitation of these vulnerabilities could allow attackers to:
  - Gain control of the kernel
  - Execute arbitrary code
  - Achieve a complete system compromise
  - Obtain root privileges
- Proof-of-concept (PoC) exploit code is publicly available for both vulnerabilities, increasing the risk of active exploitation.
- Affected Versions: > v4.18

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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://github.com/google/security-research/security/advisories/GHSA-cqc2-6j63-6qrx
- https://github.com/google/security-research/security/advisories/GHSA-fphp-6498-x998