مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Linux Kernel SMB Server Vulnerabilities

Tracking #:432316804

Date:29-01-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed critical vulnerabilities in KSMBD, the in-kernel SMB server for Linux. These vulnerabilities pose significant risks to system security and could potentially allow attackers to gain control of vulnerable systems.

TECHNICAL DETAILS:

Vulnerabilities Details:

- CVE-2024-56626
  - CVSS 9.8 Critical
  - This vulnerability is an out-of-bounds write flaw in the ksmbd_vfs_stream_write function, which handles writing data to files with extended attributes (alternate data streams). An attacker could exploit this vulnerability to write data outside the allocated buffer, potentially leading to kernel takeover.
- CVE-2024-56627
  - CVSS 9.1 Critical
  - This vulnerability is an out-of-bounds read issue in the ksmbd_vfs_stream_read function, responsible for reading data from files with extended attributes. An attacker can exploit this vulnerability by providing a negative offset, resulting in the reading of data from memory before the start of the allocated buffer.

Exploitation of this vulnerabilities could lead to:

- **Remote Code Execution (RCE)**: Attackers with network access to SMB services can execute arbitrary code with kernel privileges.
- **Information Disclosure**: Sensitive kernel memory contents may be leaked.
- **System Compromise**: Full control over affected systems, enabling APTs, ransomware deployment, or espionage.

Affected Versions:

- Linux kernel versions > 5.15

Fixed Versions:

- Linux kernel version 6.13-rc2

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-qmm2-xfcw-4r29
- https://github.com/google/security-research/security/advisories/GHSA-gqrv-6fcf-hvv8