مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# High-Severity Vulnerability in Linux Kernel

Tracking #:432317011

Date:29-03-2025

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed A heap overflow vulnerability in the Linux kernel's HFS+ file system implementation, affecting Ubuntu systems. This flaw allows local attackers to escalate privileges, potentially leading to arbitrary code execution or denial of service (system crash).

## TECHNICAL DETAILS:

**Vulnerability Details:**

- **CVE-2025-0927**
- CVSS Score 7.8 High
- A heap overflow vulnerability in the HFS+ file system implementation within the Linux kernel. This flaw resides in the hfs_bnode_read_key function located in fs/hfsplus/bnode.c. The function lacks proper boundary checks when processing B-tree node keys, allowing an attacker to potentially overwrite kernel memory.
- The vulnerability stems from the assumption that the hfs_bnode_read_key function would only be called in contexts where key lengths had been previously validated. This assumption is incorrect, leading to a buffer overflow when processing specially crafted HFS+ file systems.
- A public proof-of-concept (PoC) exploit is available, increasing the risk of widespread exploitation.
- A successful exploitation of this vulnerability could lead to:
    - Local privilege escalation
    - Denial of Service (DoS) via system crashes
    - Arbitrary code execution under elevated privileges

**Affected Systems:**

- **Ubuntu 22.04** (Default kernel version 6.5.0-18-generic)
- **Linux Kernel versions up to 6.12.0**

## RECOMMENDATIONS:

- **Apply Kernel Updates:** Install the latest security patches from Ubuntu's official repositories.
- **Restrict Mounting Permissions:** If feasible, restrict unprivileged users from mounting file systems using polkit rules or disabling loop device access.
- **Monitor System Logs:** Keep an eye on system logs for suspicious mount attempts and abnormal crashes.
- **Disable HFS+ Support if Unused:** If HFS+ file systems are not needed, consider disabling the kernel module to mitigate exposure.

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-2025-0927