مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Apple macOS Kernel

Tracking #:432316817

Date:03-02-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability (CVE-2025-24118) has been discovered in Apple's macOS kernel (XNU), allowing local attackers to escalate privileges, corrupt memory, and potentially execute code with kernel-level permissions.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2025-24118) has been discovered in Apple's macOS kernel (XNU), allowing local attackers to escalate privileges, corrupt memory, and potentially execute code with kernel-level permissions.

Key Details

- Vulnerability: Race condition in macOS kernel (XNU)
- CVE ID: **CVE-2025-24118**
- CVSS Score: **9.8** (Critical)
- Affected Systems: macOS Sonoma, macOS Sequoia, iPadOS
- Vulnerability Mechanism: The flaw arises from the interaction of Safe Memory Reclamation (SMR), per-thread credentials, read-only page mappings, and memcpy behavior.
- Attack Vector: An unprivileged local attacker can trigger the vulnerability using a multi-threaded attack that forces frequent credential updates.
- Patched Versions: macOS Sonoma 14.7.3, macOS Sequoia 15.3, iPadOS 17.7.4
- Exploit Availability: A proof-of-concept (PoC) exploit demonstrating the vulnerability has been released

RECOMMENDATIONS:

- Immediate System Updates: Organizations and individual users should immediately update their macOS and iPadOS systems to the latest versions.
- Organizations should monitor their systems for unusual activity or signs of privilege escalation.

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-2025-24118