مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Multiple Vulnerabilities in Apache NuttX RTOS Filesystem

Tracking #:432318204

Date:02-01-2026



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed The Apache Software Foundation has released security updates addressing two vulnerabilities in Apache NuttX RTOS.

## TECHNICAL DETAILS:

The Apache Software Foundation has released security updates addressing two vulnerabilities in Apache NuttX RTOS, a real-time operating system widely deployed across embedded and IoT environments. The identified issues affect the virtual filesystem (VFS) layer and could allow remote attackers to cause memory corruption, unexpected filesystem behavior, or system crashes, particularly when filesystem services are exposed over the network (e.g., FTP).

- CVE-2025-48769 – Moderate severity Use After Free vulnerability leading to heap corruption
- CVE-2025-48768 – Low severity logic flaw enabling root filesystem inode removal, causing denial of service

**Fixed Versions**

- Upgrade to version 12.11.0 or later to remediate CVE-2025-48769
- Upgrade to version 12.10.0 or later to remediate CVE-2025-48768

## RECOMMENDATIONS:

- Upgrade Apache NuttX RTOS to fixed version.

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://lists.apache.org/thread/0rs1tcj7pld0porfvyqvzpmkqswoqykc
- https://lists.apache.org/thread/7m83v11ldfq7bvw72n9t5sccocczocjn