مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Wireshark

Tracking #:432318469

Date:27-02-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Wireshark has been released security updates to remediate multiple security vulnerabilities that could allow denial-of-service (DoS) conditions via crafted packet captures or malicious live traffic.

TECHNICAL DETAILS:

Wireshark version 4.6.4 has been released to remediate multiple security vulnerabilities that could allow denial-of-service (DoS) conditions via crafted packet captures or malicious live traffic.

1. CVE-2026-3201 – USB HID Dissector Memory Exhaustion

- **Component:** USB HID dissector
- **Issue Type:** Uncontrolled sequential memory allocation
- **Impact:** Denial of Service (DoS)

2. CVE-2026-3202 – NTS-KE Dissector NULL Pointer Dereference

- **Component:** NTS-KE (Network Time Security – Key Establishment) dissector
- **Issue Type:** NULL pointer dereference
- **Impact:** Application crash

3. CVE-2026-3203 – RF4CE Profile Dissector Crash

- **Component:** RF4CE Profile dissector (Zigbee RF for Consumer Electronics)
- **Issue Type:** Crash during packet dissection
- **Impact:** Denial of Service

Fixed Versions

- Wireshark 4.6.4

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update Wireshark to the fixed or latest 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://www.wireshark.org/docs/relnotes/wireshark-4.6.4.html