

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



High-Severity Vulnerability in Wireshark

Tracking #:432317361

Date:10-06-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in Wireshark that could be exploited to trigger a denial-of-service (DoS) condition on affected systems.

TECHNICAL DETAILS:

A high-severity vulnerability, CVE-2025-5601, has been disclosed affecting multiple versions of Wireshark, a widely used network protocol analyzer. The flaw, referred to as “Dissection engine crash”, resides in the column utility module and can cause denial of service (DoS) via memory corruption during packet dissection.

Vulnerability Details:

- **CVE-2025-5601**
- CVSS Score 7.8 High
- The vulnerability stems from unsafe buffer copy operations in Wireshark’s column utility module, where input size is not adequately checked. This may result in application crashes due to memory corruption. The flaw can be triggered both during live packet capture and offline analysis of capture files

Affected Versions:

- Wireshark 4.4.0 to 4.4.6, 4.2.0 to 4.2.11

Fixed Versions:

- Wireshark 4.4.7, 4.2.12 or later.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Wireshark.

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-2025-5601>