

**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS
& DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380



**GOUVERNEMENT DE LA
REPUBLIQUE DU VANUATU**

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE
COMMUNICATION ET DE
TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

31 August 2026

Advisory 212: Wireshark Multiple Protocol Dissector Denial-of-Service Vulnerabilities (CVE-2026-76886, CVE-2026-76888).

Release Date: 24th August 2026

Impact: **CRITICAL**

TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to network and security administrators, analysts, and incident responders who use Wireshark for packet capture and analysis. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-76886 and CVE-2026-76888 are two separate crash vulnerabilities in Wireshark, the widely used open-source network protocol analyser. CVE-2026-76886 (CVSS 9.8, Critical) affects the C12.22 protocol dissector, used for ANSI smart-metering traffic. CVE-2026-76888 (CVSS 7.5, High) affects the RDP protocol dissector.

In both cases, a malformed packet - encountered in a live capture or opened from a saved capture file. This causes the relevant dissector to crash the Wireshark process, a denial of service rather than code execution. Wireshark's own advisories (wnpa-sec-2026-67 and wnpa-sec-2026-75) report no evidence of active exploitation.

What are the systems affected?

The following software and version(s) are affected:

- Wireshark versions prior to 4.6.8 (4.6.x branch) – (Affected)
- Wireshark versions prior to 4.4.18 (4.4.x branch) – (Affected)

Wireshark 4.6.8 and 4.4.18 correct both issues.

- Wireshark 4.6.8 and 4.4.18 and later – (Not affected, patched)

A crash during live capture or analysis of a malicious pcap file can interrupt a security investigation or network diagnostic session at a critical moment, which is the primary operational risk here rather than data compromise.

What does this mean?

Typical attack flow:

1. **Attacker crafts a malformed packet or capture file**
 - The attacker crafts network traffic using the C12.22 or RDP protocol, or a .pcap/.pcapng file containing such traffic, designed to trigger the flawed dissector.
2. **Victim analyses the traffic or file**
 - The victim is actively capturing matching live traffic, or opens the malicious capture file in a vulnerable Wireshark version, causing the dissector — and Wireshark itself — to crash.

Attack vectors:

- Malicious network traffic captured live on a monitored segment
- A malicious capture file shared with an analyst for review

Successful exploitation allows attackers to:

- Crash an analyst's Wireshark session (denial of service)
- Disrupt an active incident investigation or network troubleshooting effort at a time chosen by the attacker

Mitigation process

CERTVU recommends the following:

1. Upgrade Wireshark Immediately

- Update to Wireshark 4.6.8 or 4.4.18, whichever branch you run.
- Restart any active capture sessions after upgrading.

2. If immediate upgrade is not possible, disable the C12.22 and RDP dissectors as an interim workaround (Analyze > Enabled Protocols in Wireshark).
3. Handle Untrusted Capture Files with Care
 - Treat capture files from unknown or untrusted sources as potentially malicious, and analyse them on a patched, isolated system where practical.
4. Confirm the Wireshark version in use across your incident-response and network-operations toolset.
5. Monitor Wireshark's security advisories page for further updates.

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. <https://www.wireshark.org/security/wnpa-sec-2026-75.html>
2. <https://www.wireshark.org/security/wnpa-sec-2026-67.html>