مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Zoom Workplace

Tracking #:432319306

Date:17-07-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Zoom has disclosed a critical security vulnerability affecting Zoom Workplace for Windows and the Zoom Workplace VDI Client for Windows.

TECHNICAL DETAILS:

Zoom has disclosed a critical security vulnerability, CVE-2026-53412 (CVSS v3.1: 9.8 – Critical), affecting Zoom Workplace for Windows and the Zoom Workplace VDI Client for Windows. The vulnerability results from improper input validation and could allow an unauthenticated remote attacker to compromise user accounts without requiring valid credentials, user interaction, or local system access.

Vulnerability Details:

- CVE ID: CVE-2026-53412
- CVSS v3.1 Score: 9.8 (Critical)
- Product: Zoom Workplace for Windows and Zoom Workplace VDI Client for Windows
- Advisory: ZSB-26014
- Vulnerability Type: Improper Input Validation
- CWE: CWE-20 – Improper Input Validation
- The advisory was first published on 14 July 2026 and revised on 15 July 2026 to clarify that the Zoom Meeting SDK for Windows is not affected.

Affected Products:

- Zoom Workplace for Windows before version 7.0.0
- Zoom Workplace VDI Client for Windows before version 7.0.10 and 6.6.15 and 6.5.18 in their respective branches

RECOMMENDATIONS:

Immediate Actions:

- Upgrade Zoom Workplace & Zoom Workplace VDI Client for Windows to fixed version or later.

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.zoom.com/en/trust/security-bulletin/zsb-26014/