مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates – Zoom Clients

Tracking #:432317472

Date:10-07-2025

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 INTELLGIENCE 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 that Zoom Video Communications, Inc. has disclosed six new vulnerabilities affecting various Zoom Clients and the Zoom Workplace application across Windows, macOS, iOS, and Linux platforms.

TECHNICAL DETAILS:

Zoom Video Communications, Inc. has disclosed six new vulnerabilities affecting various Zoom Clients and the Zoom Workplace application across Windows, macOS, iOS, and Linux platforms. These vulnerabilities include buffer overflows, improper authentication, cross-site scripting, and certificate validation flaws. Exploitation could result in arbitrary code execution, session hijacking, or bypassing of security controls.

Of particular concern is CVE-2025-46788, a high-severity certificate validation flaw in Zoom Workplace for Linux, which may allow attackers to impersonate trusted services or perform man-in-the-middle (MITM) attacks

Two Classic Buffer Overflow vulnerabilities in Zoom Clients for Windows (ZSB-25024 and ZSB-25028) can be exploited by a local or network-accessible attacker to cause Denial-of-Service (DoS), crashing the client or freezing video services. These flaws do not require elevated privileges but do require access to the network session.

Title	CVE ID	Severity
Zoom Clients for Windows - Classic Buffer Overflow	CVE-2025-49465	Medium
Zoom Clients for macOS - Improper Authentication	CVE-2025-49464	Medium
Zoom Clients for iOS - Insufficient Control Flow Management	CVE-2025-49463	Medium
Zoom Clients - Cross-site Scripting	CVE-2025-49462	Low
Zoom Clients for Windows - Classic Buffer Overflow	CVE-2025-46789	Medium
Zoom Workplace for Linux - Improper Certificate Validation	CVE-2025-46788	High

RECOMMENDATIONS:

- **Update Zoom Clients Immediately**:
  - Windows, macOS, iOS, Linux users should upgrade to fixed version
- **Enable Auto-Updates**:
  - Ensure organization-wide policy enables automatic patching or alerts for third-party apps.

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/