مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates - Zoom

Tracking #:432317995

Date:12-11-2025

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 has released security updates to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

Zoom has released security updates to address several high and medium severity vulnerabilities across Zoom Workplace Clients, Android, Windows, macOS, and VDI products. These vulnerabilities could allow attackers to execute arbitrary code, bypass authorization, or access sensitive information.

High-Severity Vulnerabilities

- **CVE-2025-62484** – Zoom Workplace Clients: Inefficient Regular Expression Complexity
- **CVE-2025-64741** – Zoom Workplace for Android: Improper Authorization Handling
- **CVE-2025-64740** – Zoom Workplace VDI Client for Windows: Improper Verification of Cryptographic Signature

Medium-Severity Vulnerabilities

- **CVE-2025-62483** – Zoom Clients: Improper Removal of Sensitive Information
- **CVE-2025-62482** – Zoom Workplace for Windows: Cross-site Scripting
- **CVE-2025-30662** – Zoom Workplace VDI Plugin macOS Universal Installer: Symlink Following
- **CVE-2025-30669** – Zoom Workplace Clients: Improper Certificate Validation
- **CVE-2025-64739** – Zoom Clients: External Control of File Name or Path
- **CVE-2025-64738** – Zoom Workplace for macOS: External Control of File Name or Path
- **CVE-2025-30670, CVE-2025-30671 –** Zoom Workplace Apps for Windows: Null Pointer Dereference

Impact

Successful exploitation of these vulnerabilities could result in unauthorized access, arbitrary code execution, sensitive data exposure, or denial of service. Attackers may also gain elevated privileges or compromise the integrity and confidentiality of affected systems.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update Zoom to the 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.zoom.com/en/trust/security-bulletin/