

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Privilege Escalation Vulnerability in Zoom

Tracking #:432317596

Date:13-08-2025

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 multiple vulnerabilities in Zoom Clients for Windows that could potentially be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

1. CVE-2025-49457

- **CVSS Score:** 9.6 **Critical**
- A critical vulnerability exists in certain Zoom Clients for Windows that could allow an unauthenticated attacker to escalate privileges via network access. The flaw stems from an untrusted search path, which could be exploited to execute malicious code in the context of the vulnerable application.
- **Affected Products:**
 - Zoom Workplace for Windows before version 6.3.10
 - Zoom Workplace VDI for Windows before version 6.3.10 (except 6.1.16 and 6.2.12)
 - Zoom Rooms for Windows before version 6.3.10
 - Zoom Rooms Controller for Windows before version 6.3.10
 - Zoom Meeting SDK for Windows before version 6.3.10

2. CVE-2025-49456

- **CVSS Score:** 6.2 Medium
- A race condition vulnerability exists in the installer of certain Zoom Clients for Windows. An attacker with local access could exploit this flaw to manipulate application files or configurations, resulting in unauthorized modifications.
- **Affected Products:**
 - Zoom Workplace for Windows version 6.4.10
 - Zoom Workplace VDI for Windows before version 6.3.12 (except 6.2.15)
 - Zoom Rooms for Windows before version 6.4.5
 - Zoom Rooms Controller for Windows before version 6.4.5
 - Zoom Meeting SDK for Windows before version 6.4.10

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by ZOOM.

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-25030/>
- <https://www.zoom.com/en/trust/security-bulletin/zsb-25029/>