



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Information Disclosure Vulnerability in Multiple Zoom Products

Tracking #:432316289

Date:16-09-2024

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 a medium-severity vulnerability has been identified in the Zoom Workplace Apps, specifically a business logic error that may allow unauthenticated users to disclose sensitive information through network access.

TECHNICAL DETAILS:

A medium-severity vulnerability has been identified in the Zoom Workplace Apps, specifically a business logic error that may allow unauthenticated users to disclose sensitive information through network access. This vulnerability, cataloged as CVE-2024-45424, affects multiple platforms and could potentially expose users to data breaches if not addressed promptly.

- **CVE ID:** CVE-2024-45424
- **CVSS Severity:** Medium
- **CVSS Score:** 5.3
- **CVSS Vector String:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Affected Products:

- Zoom Workplace Desktop App for Windows before version 6.1.0
- Zoom Workplace Desktop App for macOS before version 6.1.0
- Zoom Workplace Desktop App for Linux before version 6.1.0
- Zoom Workplace VDI Client for Windows before version 6.1.0 (except versions 5.17.15 and 6.0.12)
- Zoom Workplace App for iOS before version 6.1.0
- Zoom Workplace App for Android before version 6.1.0
- Zoom Meeting SDK for Windows before version 6.1.0
- Zoom Meeting SDK for iOS before version 6.1.0
- Zoom Meeting SDK for Android before version 6.1.0
- Zoom Meeting SDK for macOS before version 6.1.0
- Zoom Meeting SDK for Linux before version 6.1.0
- Zoom Rooms App for Windows before version 6.1.0
- Zoom Rooms App for macOS before version 6.1.0
- Zoom Rooms App for iPad before version 6.1.0
- Zoom Rooms Controller for Windows before version 6.1.0
- Zoom Rooms Controller for macOS before version 6.1.0
- Zoom Rooms Controller for Linux before version 6.1.0
- Zoom Rooms Controller for Android before version 6.1.0

**RECOMMENDATIONS:**

The UAE Cyber Security Council recommends to upgrade to the latest version as soon as possible.

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-24036/>