

Overall rating: Critical



This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a vulnerability in the Zoom video conferencing software. Released security updates for seven vulnerabilities in its desktop and mobile applications (Zoom clients for Windows, macOS, Linux, Android, and iOS).

Technical Details

There are two vulnerabilities that are particularly noteworthy, the critical CVE-2024-24691 (CVSS score of 9.6) and the high-severity CVE-2024-24697 (7.2) which could enable privilege escalation for unauthenticated users via network access and for authenticated user via local access, due to an input validation issue and an untrusted search path issue in Zoom Desktop Client, Zoom VDI Client, Zoom Rooms Client, and Zoom Meeting SDK for Windows. Zoom also addressed the following vulnerabilities in its latest release which may allow threat actors to conduct DDoS attack, information disclosure against vulnerable clients:

- CVE-2024-24690: Improper Input Validation in Zoom Clients for various OS's
- CVE-2024-24699: Business Logic Error in Zoom Clients for various OS's
- CVE-2024-24698: Improper Authentication in Zoom Clients for various OS's
- CVE-2024-24696: Improper Input Validation in Zoom clients for Windows
- CVE-2024-24695: Improper Input Validation in Zoom Clients for Windows

Exploitability Metrics

Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify [VRM](#) with any questions or concerns you may have.

References

- [Zoom Patches Critical Vulnerability in Windows Applications - SecurityWeek](#)
- [Zoom Security Bulletins | Zoom](#)
- [Zoom stomps critical privilege escalation bug, 6 other flaws • The Register](#)

- [Zoom patches critical privilege elevation flaw in Windows apps \(bleepingcomputer.com\)](https://www.bleepingcomputer.com/news/security/zoom-patches-critical-privilege-elevation-flaw-in-windows-apps/)