August 16, 2024

Overall Rating: High

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a Zoom Security bulletin. The vulnerability affects Zoom Workplace Desktop App for Windows, macOS and Linux before version 6.0.0, Zoom Workplace VDI Client for Windows before version 5.17.13, Zoom Workplace App for iOS and App for Android before version 6.0.0 and Zoom Rooms App for Windows, App for Mac and App for iPad before version 6.0.0.

Technical Details

ZSB	Title	Severity	CVE
ZSB-24035	Zoom Workplace Desktop App for Linux - Improper Input Validation	Medium	CVE-2024-42443
ZSB-24034	Zoom Workplace Desktop App for macOS, Zoom Meeting SDK for macOS, Zoom Rooms Client for macOS - Improper Privilege Management	Medium	CVE-2024-42441, CVE-2024-42442
ZSB-24033	Zoom Workplace Apps and SDKs - Buffer Overflow	Medium	CVE-2024-42439
ZSB-24032	Zoom Workplace Desktop App for macOS and Zoom Meeting SDK for macOS - Untrusted Search Path	Medium	CVE-2024-42440
ZSB-24031	Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controller - Buffer Overflow	Medium	CVE-2024-42436, CVE-2024-42437, CVE-2024-42438
ZSB-24030	Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers - Sensitive Information Exposure	Medium	CVE-2024-39823, CVE-2024-39824, CVE-2024-42434, CVE-2024-42435
ZSB-24029	Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers - Sensitive Information Exposure	Medium	CVE-2024-39822
ZSB-24025	Zoom Workplace Apps and SDKs - Protection Mechanism Failure	High	CVE-2024-39818
ZSB-24022	Zoom Workplace Apps and Rooms Clients - Buffer Overflow	High	CVE-2024-39825

Buffer overflow in some Zoom Workplace Apps and Rooms Clients may allow an authenticated user to conduct an escalation of privilege via network access. Additionally, Protection mechanism failure in some Zoom Workplace Apps and SDKs may allow an authenticated user to conduct information disclosure via network access.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: High
Privileges Required: Low
User Interaction: None

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

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 at VulnerabilityandRiskManagement@gov.bc.ca.

References

CVE

- Zoom Security Bulletins
- VRM Vulnerability Reports