Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Flaw in Zoom Windows Apps Allows Privilege Elevation

Date of Publication	Admiralty Code	TA Number
February 15, 2024	A1	TA2024059

Summary

First Seen: February 13, 2024
Affected Products: Zoom desktop and VDI clients, Zoom Rooms Client and the Meeting SDK for Windows
Impact: Zoom has addressed an input validation flaw (CVE-2024-24691) that renders the Zoom desktop and VDI clients, along with the Meeting SDK for Windows, vulnerable to privilege escalation on the target system via the network, even by an unauthenticated attacker.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-24691	Zoom Improper Input Validation Vulnerability	Zoom Desktop Client, Zoom VDI Client, Zoom Rooms Client and Zoom Meeting SDK for Windows	✗	✗	✓
CVE-2024-24697	Zoom Untrusted Search Path Vulnerability	Zoom Desktop Client, Zoom VDI Client, Zoom Rooms Client and Zoom Meeting SDK for Windows	✗	✗	✓

Vulnerability Details

#1 Zoom has addressed a critical issue, identified as CVE-2024-24691, characterized as improper input validation. This vulnerability could enable an attacker with network access to escalate privileges, impacting Zoom desktop and VDI clients, as well as the Meeting SDK for Windows.

#2 The compromised machine can be remotely accessed by attackers by exploiting CVE-2024-24691. The lack of proper validation of user-supplied input is the cause of this vulnerability. Malicious links can be used to lure users into clicking on them, giving attackers access to the system.

#3 Furthermore, Zoom has addressed CVE-2024-24697, another high-severity vulnerability, in its latest release. This bug affects Zoom's 32-bit Windows clients and enables privilege escalation through local access by exploiting an untrusted search path.

#4 Additionally, the company cautioned about multiple medium-severity vulnerabilities in the Zoom clients for desktop and mobile platforms, which could be exploited for conducting denial-of-service attacks or leaking information. To mitigate the risk of external actors gaining elevated privileges, installing backdoors, disrupting or eavesdropping on meetings, and stealing sensitive data, it is highly recommended that Zoom users promptly apply the security update.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-24691	Zoom Desktop Client for Windows before version 5.16.5 Zoom VDI Client for Windows before version 5.16.10 (excluding 5.14.14 and 5.15.12) Zoom Rooms Client for Windows before version 5.17.0 Zoom Meeting SDK for Windows before version 5.16.5	cpe:2.3:a:zoom:*:*:*:*:*:*	CWE-20
CVE-2024-24697	Zoom Desktop Client for Windows before version 5.17.0 Zoom VDI Client for Windows before version 5.17.5 (excluding 5.15.15 and 5.16.12) Zoom Meeting SDK for Windows before version 5.17.0 Zoom Rooms Client for Windows before version 5.17.0	cpe:2.3:a:zoom:*:*:*:*:*:*	CWE-426

Recommendations

Apply Patch: Install the security patch provided by Zoom to address the CVE-2024-24691 and CVE-2024-24697 vulnerabilities. This patch closes the security gap that allows attackers to exploit the vulnerability.

Least Privilege: Adhere to the idea of "least privilege" by giving users/ application only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application	T1566 Phishing	T1566.002 Spearphishing Link
T1204 User Execution	T1204.001 Malicious Link	T1203 Exploitation for Client Execution	

Patch Details

Zoom has released patches to address the vulnerability in the latest Version

Link:
https://zoom.us/download

References

https://www.zoom.com/en/trust/security-bulletin/ZSB-24008/

https://www.zoom.com/en/trust/security-bulletin/ZSB-24004/

https://www.hkcert.org/security-bulletin/zoom-products-multiple-vulnerabilities_20240214

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.

Contextualize
Uni5 Threat Exposure Management
Resolve
Prioritize

REPORT GENERATED ON

February 15, 2024 • 4:45 AM

More at www.hivepro.com