

Cybersecurity Threat Intelligence

Written by Tyler Weiss

Assignment

This assignment involves analyzing a specific CVE for Zoom from 2/14/24 to understand real-world cybersecurity threat intelligence (CTI). You'll gather information on this CVE, focusing on the vulnerability, advisories, remediation steps, and relevant data.

For this assignment:

1. Find and take screenshots of the CVE details, the official advisory, the recommended fixes, and any extra useful information.
2. Write a brief explanation of CTI's role and importance in cybersecurity.
3. Craft an executive summary about the CVE for management, keeping it clear and non-technical, followed by a section with more technical details for those interested.

Step 1

Find and take screenshots of the CVE details, the official advisory, the recommended fixes, and any extra useful information.

Zoom Desktop Client for Windows, Zoom VDI Client for Windows, and Zoom Meeting SDK for Windows - Improper Input Validation
CVE-2024-24691

Official Zoom Security Bulletin

<https://www.zoom.com/en/trust/security-bulletin/zsb-24008/>

CVSS: 9.6

Severity: Critical

The critical vulnerability affects the following Zoom products and versions:

- 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 Meeting SDK for Windows before version 5.16.5
- Zoom Rooms Client for Windows before version 5.17.0

Users can help keep themselves secure by applying the latest updates available at <https://zoom.us/download>.

Zoom Desktop Client for Windows, Zoom VDI Client for Windows, and Zoom Meeting SDK for Windows – Improper Input Validation

Bulletin: ZSB-24008

CVEID: CVE-2024-24691

CVSS Severity: Critical

CVSS Score: 9.6

CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Description:

Improper input validation in Zoom Desktop Client for Windows, Zoom VDI Client for Windows, and Zoom Meeting SDK for Windows may allow an unauthenticated user to conduct an escalation of privilege via network access.

Users can help keep themselves secure by applying the latest updates available at <https://zoom.us/download>.

Affected Products:

- 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

Source:

Reported by Zoom Offensive Security.

NIST CVE Database

<https://nvd.nist.gov/vuln/detail/CVE-2024-24691>

CVE-2024-24691 Detail

AWAITING ANALYSIS

This vulnerability is currently awaiting analysis.


Description

Improper input validation in Zoom Desktop Client for Windows, Zoom VDI Client for Windows, and Zoom Meeting SDK for Windows may allow an unauthenticated user to conduct an escalation of privilege via network access.

Severity


CVSS Version 3.xCVSS Version 2.0

CVSS 3.x Severity and Metrics:

 **NIST:** NVD

Base Score: N/A

NVD assessment not yet provided.

 **CNA:** Zoom Video Communications, Inc.

Base Score: 9.6 CRITICAL

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

QUICK INFO


CVE Dictionary Entry:
CVE-2024-24691
NVD Published Date:
02/13/2024
NVD Last Modified:
02/14/2024
Source:
Zoom Video Communications, Inc.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

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

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-20	Improper Input Validation	 Zoom Video Communications, Inc.

CWE-20 MITRE Improper Input Validation
<https://cwe.mitre.org/data/definitions/20.html>

CWE-20: Improper Input Validation

Weakness ID: 20

Vulnerability Mapping: **DISCOURAGED**

Abstraction: Class

View customized information:

Conceptual

Operational

Mapping Friendly

Complete

Custom

Description

The product receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly.

Extended Description

Input validation is a frequently-used technique for checking potentially dangerous inputs in order to ensure that the inputs are safe for processing within the code, or when communicating with other components. When software does not validate input properly, an attacker is able to craft the input in a form that is not expected by the rest of the application. This will lead to parts of the system receiving unintended input, which may result in altered control flow, arbitrary control of a resource, or arbitrary code execution.
Input validation is not the only technique for processing input, however. Other techniques attempt to transform potentially-dangerous input into something safe, such as filtering ([CWE-790](#)) - which attempts to remove dangerous inputs - or encoding/escaping ([CWE-116](#)), which attempts to ensure that the input is not misinterpreted when it is included in output to another component. Other techniques exist as well (see [CWE-138](#) for more examples.)
Input validation can be applied to:

- raw data - strings, numbers, parameters, file contents, etc.
- metadata - information about the raw data, such as headers or size

Tenable CVE Database
<https://www.tenable.com/cve/CVE-2024-24691>

CVE-2024-24691

CRITICAL

Information

CPEs

Plugins

Description

Improper input validation in Zoom Desktop Client for Windows, Zoom VDI Client for Windows, and Zoom Meeting SDK for Windows may allow an unauthenticated user to conduct an escalation of privilege via network access.

References

https://www.theregister.com/2024/02/15/zoom_privilege_escalation/
<https://www.hivepro.com/threat-advisory/critical-flaw-in-zoom-windows-apps-allows-privilege-elevation/>
https://www.bleepingcomputer.com/news/security/zoom-patches-critical-privilege-elevation-flaw-in-windows-apps/?web_view=true
<https://www.bleepingcomputer.com/news/security/zoom-patches-critical-privilege-elevation-flaw-in-windows-apps/>
<https://www.securityweek.com/zoom-patches-critical-vulnerability-in-windows-applications/>
<https://www.zoom.com/en/trust/security-bulletin/ZSB-24008/>

Details

Source: [Mitre](#), [NVD](#)

Published: 2024-02-14

Updated: 2024-02-14

Risk Information

CVSS v2

Base Score: 10

Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Severity: Critical

CVSS v3

Base Score: 9.6

Vector:

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Severity: Critical

Tenable References:

https://www.theregister.com/2024/02/15/zoom_privilege_escalation/
<https://www.hivepro.com/threat-advisory/critical-flaw-in-zoom-windows-apps-allows-privilege-elevation/>
https://www.bleepingcomputer.com/news/security/zoom-patches-critical-privilege-elevation-flaw-in-windows-apps/?web_view=true
<https://www.bleepingcomputer.com/news/security/zoom-patches-critical-privilege-elevation-flaw-in-windows-apps/>
<https://www.securityweek.com/zoom-patches-critical-vulnerability-in-windows-applications/>
<https://www.zoom.com/en/trust/security-bulletin/ZSB-24008/>

Rapid7 Vulnerability Database

<https://www.rapid7.com/db/vulnerabilities/zoom-zoom-cve-2024-24691/>

Zoom: CVE-2024-24691: Zoom Desktop Client for Windows, Zoom VDI Client for Windows, and Zoom Meeting SDK for Windows - Improper Input Validation

Severity	CVSS	Published	Created	Added	Modified
10	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	02/13/2024	02/20/2024	02/16/2024	02/21/2024

Description

Improper input validation in Zoom Desktop Client for Windows, Zoom VDI Client for Windows, and Zoom Meeting SDK for Windows may allow an unauthenticated user to conduct an escalation of privilege via network access. Users can help keep themselves secure by applying the latest updates available at <https://zoom.us/download>.

Solution(s)

zoom-zoom-upgrade-latest

References

- <https://attackerkb.com/topics/cve-2024-24691>
- <https://www.zoom.com/en/trust/security-bulletin/>
- [CVE - 2024-24691](#)

CVE Details Database
Exploitability Score: 2.8
Impact Score: 6.0
Attack Vector: Network
Attack Complexity: Low
Privilege Requirements: None
User Interaction: Required
Confidentiality: High
Integrity: High
Availability: High

Vulnerability Details : CVE-2024-24691

Improper input validation in Zoom Desktop Client for Windows, Zoom VDI Client for Windows, and Zoom Meeting SDK for Windows may allow an unauthenticated user to conduct an escalation of privilege via network access.

Published 2024-02-14 00:15:47 Updated 2024-02-14 00:15:47 Source [Zoom Video Communications, Inc.](#) View at [NVD](#), [CVE.org](#)

Vulnerability category: [Input validation](#)

Exploit prediction scoring system (EPSS) score for CVE-2024-24691

Probability of exploitation activity in the next 30 days:

0.04%

Percentile, the proportion of vulnerabilities that are scored at or less:

~ 7 %

[EPSS Score History](#) [EPSS FAQ](#)

CVSS scores for CVE-2024-24691

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source		
9.6	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H	2.8	6.0	Zoom Video Communications, Inc.		
Attack Vector: Network	Attack Complexity: Low	Privileges Required: None	User Interaction: Required	Scope: Changed	Confidentiality: High	Integrity: High	Availability: High

Step 2

Write a brief explanation of Cybersecurity Threat Intelligence's (CTI) role and importance in cybersecurity.

CTI is crucial to for businesses and cyber professionals to make informed decisions and reduce the risk of cyber attacks. The sharing of threat information allows cyber professionals to identify possible undetected intrusions, protect against and mitigate future threats, prioritize patching of vulnerable systems, share/create solutions and create awareness of the threat landscape. Threat feeds can also inform and provide Indicators of Compromise (IoC), Indicators of Attack (IoC), malicious URLs and IP addresses, malware signatures and other important that can be used and deployed to protect networks, systems and applications. In short the sharing of CTI provides the knowledge base necessary to protect our current cyber environments.

Step 3

Craft an executive summary about the CVE for management, keeping it clear and non-technical, followed by a section with more technical details for those interested.

A Zoom vulnerability, that effects Windows clients where Zoom is installed, may enable privilege escalation for unauthenticated users via network access meaning a threat actor could attain higher level privileges such as administrator rights by using non-valid input through Zoom software. This vulnerability is labeled as Critical, being uncomplicated to execute and severely effecting all Zoom Clients on Windows systems, requiring minimal user interaction. This update was reported by Zoom security researchers at their Offensive Security Division. No successful exploits have yet been detected in the wild. To resolve the issue download and install the update from Zoom found at <https://zoom.us/download>. Limited other details have been disclosed regarding this threat.

Zoom Desktop Client for Windows, Zoom VDI Client for Windows, and Zoom Meeting SDK for Windows - Improper Input Validation

Solution: Applying the latest updates available at <https://zoom.us/download>.

CVSS: 9.6

CVE-2024-24691

Severity: Critical

The critical vulnerability affects the following Zoom products and versions:

- 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 Meeting SDK for Windows before version 5.16.5
- Zoom Rooms Client for Windows before version 5.17.0

Exploitability Score: 2.8

Impact Score: 6.0

Attack Vector: Network

Attack Complexity: Low

Privilege Requirements: None

User Interaction: Required

Confidentiality: High

Integrity: High

Availability: High

CWE-20 MITRE Improper Input Validation:

<https://cwe.mitre.org/data/definitions/20.html>