

Name: Cristian Barreno

Cybersecurity Current Threat Intelligence – Assignment #6

02/14/2024: Zoom platform - discovered Improper Input validation vulnerability.
Common vulnerability and Exposure (CVE): CVE-2024-24691

Executive Summary: on February, 14th 2024 a vulnerability was found in the Zoom platform used to make video calls and online meetings. This vulnerability has a 9.6 critical score. Improper user input validation is a computer software vulnerability that threat actors exploit to conduct an escalation of privilege via network access. To mitigate this is required to download the latest version of Zoom before using the application again.

Technical Details: Zoom released a list of affected Zoom windows products that have a vulnerability (CVE-2024-24691) .It has a common vulnerability scoring system AKA CVSS Score of 9.6. This vulnerability has an exploitability score of 2.8. Impact score of 6.0. Improper user input validation is a computer software vulnerability that threat actors exploit to conduct an escalation of privilege via network access. Implementing updates is vital to prevent the exploitation of this vulnerability.

What is Cyber Threat Intelligence's (CTI) role and importance in cybersecurity?

Organizations use cyber threat intelligence to prevent, understand, and act upon the behaviors of cyber criminals. It allows organizations to be proactive and not reactive. There are many sources of cyber threat intelligence including past incidents, feeds, and open source information. MITRE developed the Structured Threat Information Expressions (STIX) to share threat intelligence, and also the Adversarial Tactics Techniques and Common Knowledge (ATT&CK) framework that is updated with new techniques and tactics as they emerge. Other source of cyber threat intelligence could be on your social media feed, from people that you follow that are into cybersecurity.

Zoom security bulletin:

SearchSupport1.888.799.9666Request a DemoJoinHostSign In

zoomProductsSolutionsResourcesPlans & PricingContact SalesSign Up Free

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.

Vulnerability details:

DocumentationCVE ID, product, vendorSearchLog In

CVEDetails.com
powered by SecurityScorecard

Vulnerabilities

- By Date
- By Type
- Known Exploited

Assigners

- CVSS Scores
- EPSS Scores
- Search

Vulnerable Software

- Vendors
- Products
- Version Search

Vulnerability Intel.

- Newsfeed
- Open Source Vulns
- Emerging CVEs
- Feeds
- Exploits
- Advisories
- Code Repositories
- Code Changes

Attack Surface

- My Attack Surface
- Digital Footprint
- Discovered Products
- Patent & Vulner

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: 0.00%

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	0.00	6.0	Zoom Video Communications, Inc.

CWE ids for CVE-2024-24691

CWE-20 Improper Input Validation
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.
Assigned by: security@zoom.us (Secondary)

References for CVE-2024-24691

<https://www.zoom.com/en/trust/security-bulletin/ZSB-24008/>
ZSB-24008 | Zoom

2

National Institute of Standards and Technology (NIST) National Vulnerability Database(NVD):

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.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: N/A

NVD score 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

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have not published a CVSS score for this CVE at this time. NVD Analysts use publicly available information at the time of analysis to associate CVSS vector strings. A CNA provided score within the CVE List has been displayed.

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 rvd@nist.gov.

Hypertlink	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.