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

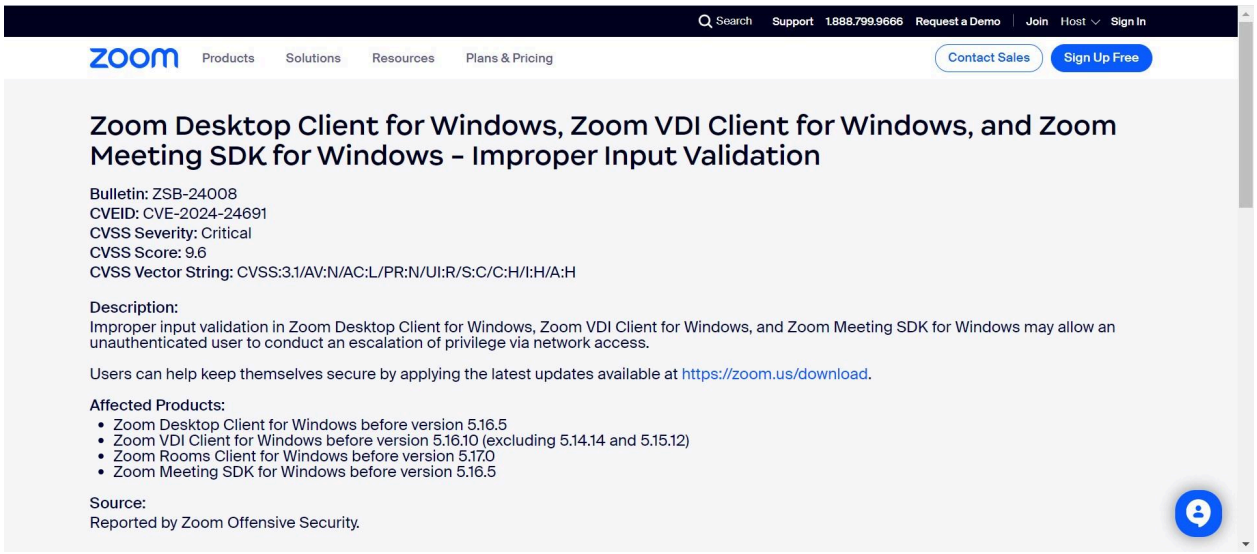
Executive Summary: on February, 14th 2024 a vulnerability was found in the Zoom platform used to make video calls and online meetings. This vulnerability has a 9.6 critical score. Improper user input validation is a computer software vulnerability that threat actors exploit to conduct an escalation of 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.

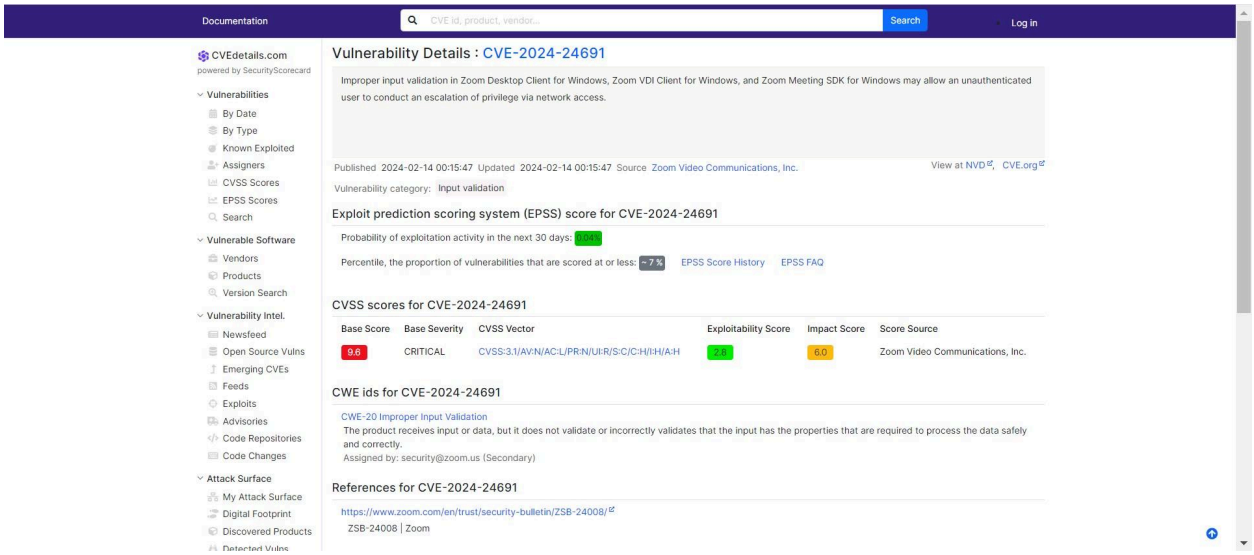
What is Cyber Threat Intelligence's (CTI) role and importance in cybersecurity?

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.

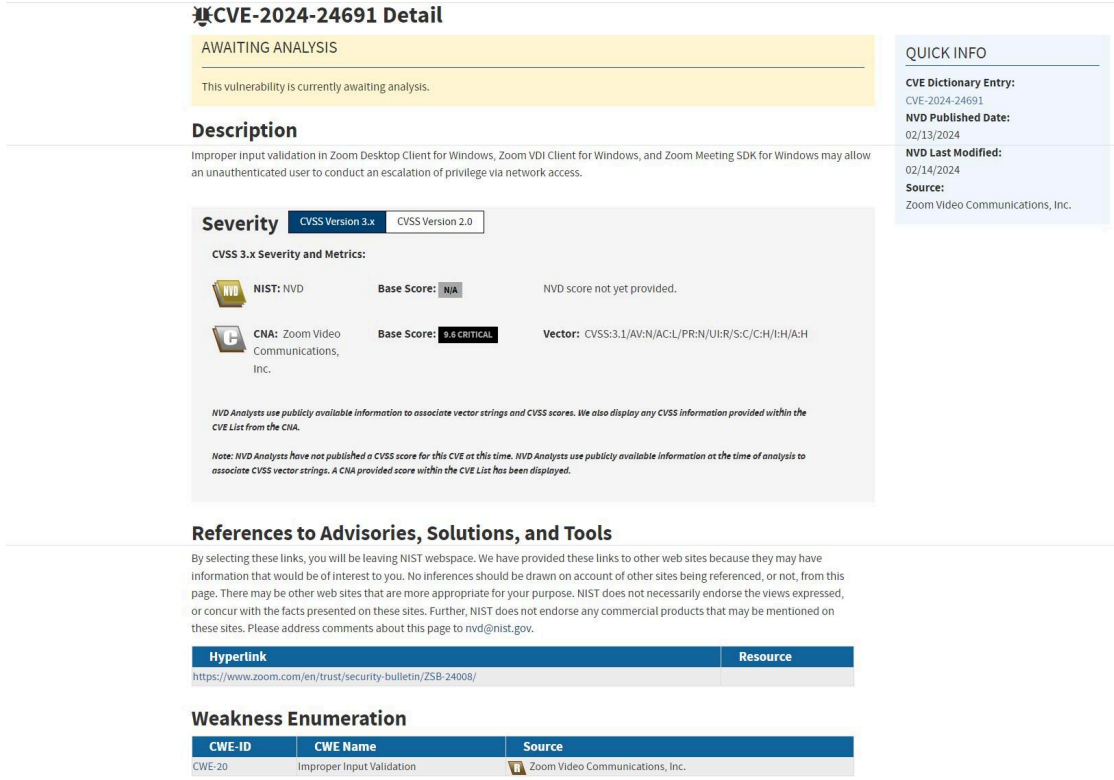
Zoom security bulletin:



Vulnerability details:



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.

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.

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 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.