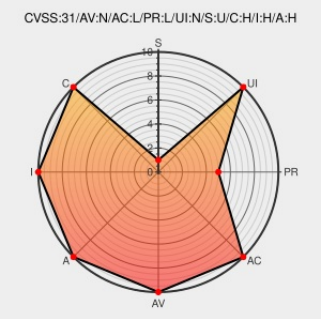
CVE-2023-36541

Published on: Not Yet Published

Last Modified on: 08/11/2023 02:09:00 PM UTC

CVE-2023-36541

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Zoom from Zoom contain the following vulnerability:

Insufficient verification of data authenticity in Zoom Desktop Client for Windows before 5.14.5 may allow an authenticated user to enable an escalation of privilege via network access.

CVE-2023-36541 has been assigned by security@zoom.us to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Zoom Video Communications, Inc.** - **Zoom Desktop Client for Windows** version **= before 5.14.5**

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Security Bulletins | Zoom	explore.zoom.us text/html	MISC explore.zoom.us/en/trust/security/security-bulletin/

Related QID Numbers

378785 Zoom Desktop Client Escalation Privilege Vulnerability (ZSB-23027)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zoom	Zoom	All	All	All	All

cpe:2.3:a:zoom:zoom:*:*:*:*:*:windows:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→