

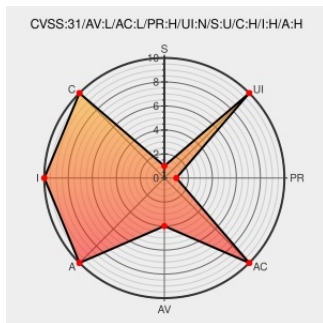


CVE-2023-39201

Published on: Not Yet Published

Last Modified on: 09/16/2023 03:30:00 AM UTC

CVE-2023-39201

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Cleanzoom](#) from [Zoom](#) contain the following vulnerability:

Untrusted search path in CleanZoom before file date 07/24/2023 may allow a privileged user to conduct an escalation of privilege via local access.

CVE-2023-39201 has been assigned by [zm](#) security@zoom.us to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [zm](#) **Zoom Video Communications, Inc. - CleanZoom** version = **before file date 07/24/2023**

CVSS3 Score: **6.7 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	HIGH	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	zm MISC explore.zoom.us/en/trust/security/security-bulletin/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites 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 websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](#).

There are currently no QIDs associated with this CVE

Known Affected Configurations (CVE V3.0)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Zoom	Cleanzoom	All	All	All	All
cpe:2.3:a:zoom:cleanzoom:*:*:*:*:*:						
No vendor comments have been submitted for this CVE						
← Previous ID				Next ID→		