



CVE-2023-22883

Published on: Not Yet Published

Last Modified on: 03/23/2023 07:27:00 PM UTC

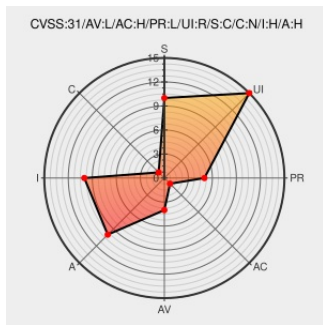
CVE-2023-22883

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Zoom Client for IT Admin Windows installers before version 5.13.5 contain a local privilege escalation vulnerability. A local low-privileged user could exploit this vulnerability in an attack chain during the installation process to escalate their privileges to the SYSTEM user.

CVE-2023-22883 has been assigned by [Z](#) security@zoom.us to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Z](#) **Zoom Video Communications Inc - Zoom Client for Meetings for IT Admin Windows installers version < 5.13.5**

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	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	Z 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.

Related QID Numbers










[378079](#) Zoom Client for Meetings Multiple Security Vulnerabilities (ZSB-23003)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zoom	Meetings	All	All	All	All
cpe:2.3:a:zoom:meetings:*:*:*:*:windows:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @ripjyr	Zoomに、Highの脆弱性情報 ZSB-23003 が公開されました。「CVE-2023-22883 : Local Privilege Escalation in Zoom for Windows Installers」 explore.zoom.us/en/trust/secur...	2023-03-14 21:53:37
 @the_yellow_fall	Zoom fixes two high-risk security CVE-2023-22885 & CVE-2023-22883 flaws securityonline.info/zoom-fixes-two... #opensource #infosec #security #pentesting	2023-03-15 10:05:03
 @AcooEdi	Zoom fixes two high-risk security CVE-2023-22885 & CVE-2023-22883 flaws dlvr.it/SkwHkJ via securityonline https://t.co/bbyC7vZzjS	2023-03-15 10:09:34
 @schectman_hell	securityonline.info/zoom-fixes-two...	2023-03-15 12:12:23
 @moton	Zoom fixes two high-risk security CVE-2023-22885 & CVE-2023-22883 flaws - securityonline.info/zoom-fixes-two...	2023-03-15 14:37:53
 @Komodosec	#Vulnerability #CVE202322880 Zoom fixes two high-risk security CVE-2023-22885 & CVE-2023-22883 flaws securityonline.info/zoom-fixes-two...	2023-03-15 15:14:04
 @rkx73	#CVE-2023-22885 #CVE-2023-22883 Dos vulnerabilidades en la aplicación Zoom permiten tomar el control de su disposit... twitter.com/i/web/status/1...	2023-03-16 20:15:50
 @CVEreport	CVE-2023-22883 : Zoom Client for IT Admin #Windows installers before version 5.13.5 contain a local privilege escal... twitter.com/i/web/status/1...	2023-03-16 21:10:40
 /r/netcve	CVE-2023-22883	2023-03-16 21:38:53

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report