



CVE-2023-36539

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-36539
State	PUBLIC
Assigner	security@zoom.us
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-30 03:15:00 UTC
Updated	2023-07-10 13:29:00 UTC
Description	Exposure of information intended to be encrypted by some Zoom clients may lead to disclosure of sensitive information.

Risk And Classification

Problem Types: CWE-326

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zoom	Meetings	5.15.0	All	All	All
Application	Zoom	Meetings	5.15.0	All	All	All
Application	Zoom	Meetings	5.15.0	All	All	All
Application	Zoom	Meetings	5.15.1	All	All	All
Hardware	Zoom	Poly Ccx 600	-	All	All	All
Operating System	Zoom	Poly Ccx 600 Firmware	5.15.0	All	All	All
Hardware	Zoom	Poly Ccx 700	-	All	All	All
Operating System	Zoom	Poly Ccx 700 Firmware	5.15.0	All	All	All
Application	Zoom	Rooms	5.15.0	All	All	All
Application	Zoom	Rooms	5.15.0	All	All	All
Application	Zoom	Rooms	5.15.0	All	All	All
Application	Zoom	Video Software Development Kit	1.8.0	All	All	All
Hardware	Zoom	Yealink Mp54	-	All	All	All
Operating System	Zoom	Yealink Mp54 Firmware	5.15.0	All	All	All
Hardware	Zoom	Yealink Mp56	-	All	All	All
Operating System	Zoom	Yealink Mp56 Firmware	5.15.0	All	All	All
Hardware	Zoom	Yealink Vp59	-	All	All	All

Operating System	Zoom	Yealink Vp59 Firmware	5.15.0	All	All	All
Application	Zoom	Zoom	5.15.0	All	All	All
Application	Zoom	Zoom	5.15.0	All	All	All
Application	Zoom	Zoom	5.15.0	All	All	All
Application	Zoom	Zoom	5.15.0	All	All	All
Application	Zoom	Zoom	5.15.1	All	All	All

References

Reference	Source	Link	Tags
Security Bulletins Zoom	MISC	explore.zoom.us	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[378723](#) Zoom Client and Rooms Information Disclosure Vulnerability (ZSB-23025)

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API cve.report/api

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