



CVE-2022-22787

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

Summary

CVE	CVE-2022-22787
State	PUBLIC
Assigner	security@zoom.us
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-18 17:15:00 UTC
Updated	2022-05-27 15:19:00 UTC
Description	The Zoom Client for Meetings (for Android, iOS, Linux, macOS, and Windows) before version 5.10.0 fails to properly validate

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Zoom XMPP Stanza Smuggling Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
Security Bulletin Zoom	CONFIRM	explore.zoom.us	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Ivan Fratric of Google Project Zero

Legacy QID Mappings

[376638](#) Zoom Client Multiple Security Vulnerabilities

[630814](#) Zoom Client for Meetings For Android Extensible Markup Language (XML) Injection Vulnerability

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)