



CVE-2020-11500

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

Summary

CVE	CVE-2020-11500
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-03 13:15:00 UTC
Updated	2020-04-07 13:46:00 UTC
Description	Zoom Client for Meetings through 4.6.9 uses the ECB mode of AES for video and audio encryption. Within a meeting, all pa

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
Move Fast and Roll Your Own Crypto: A Quick Look at the Confidentiality of Zoom Meetings - The Citizen Lab	MISC	citizenlab.ca
Zoom's Flawed Encryption Linked to China	MISC	theintercept.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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