



CVE-2021-28681

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-28681
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-18 04:15:00 UTC
Updated	2021-03-25 13:45:00 UTC
Description	Pion WebRTC before 3.0.15 didn't properly tear down the DTLS Connection when certificate verification failed. The PeerCo

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Webrtc Project	Webrtc	All	All	All	All

References

Reference	Source	Link
Failed DTLS certificate verification doesn't stop data channel communication · Advisory · pion/webrtc · GitHub	MISC	github.com
DTLS Fingerprints in SDP Offer/Answer are not verified · Issue #1708 · pion/webrtc · GitHub	MISC	github.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.

Legacy QID Mappings

982400 Go (go) Security Update for github.com/pion/webrtc/v3 (GHSA-74xm-qj29-cq8p)

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](#)