CVE-2020-12105

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2020-12105
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-23 17:15:00 UTC
Updated	2022-05-03 14:21:00 UTC
Description	OpenConnect through 8.08 mishandles negative return values from X509_check_ function calls, which might assist attacke

Risk And Classification

Problem Types: CWE-755

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Infradead	Openconnect	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

References

Reference
[security-announce] openSUSE-SU-2020:0694-1: moderate: Security update f
OpenConnect: Multiple vulnerabilities (GLSA 202006-15) — Gentoo security
incorrect use of X509_check_* functions, leading to MITM attacks. (!96) · Merge Requests · OpenConnect VPN projects / OpenConnect · GitL
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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