CVE-2022-27820

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

Summary

CVE	CVE-2022-27820
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-24 04:15:00 UTC
Updated	2022-03-31 18:59:00 UTC
Description	OWASP Zed Attack Proxy (ZAP) through w2022-03-21 does not verify the TLS certificate chain of an HTTPS server.

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Owasp	Zed Attack Proxy	All	All	All	All

References

Reference	Source	Link
Add option to allow server certificate validation (CVE-2022-27820) · Issue #7165 · zaproxy/zaproxy · GitHub	MISC	github.com
oss-security - Re: Lack of TLS certification chain validation in ZAP Proxy	MLIST	www.openwall.co
oss-security - Lack of TLS certification chain validation in ZAP Proxy	MISC	www.openwall.co
Releases · zaproxy/zaproxy · 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.

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