CVE-2022-41912

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

Summary

CVE	CVE-2022-41912
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-28 15:15:00 UTC
Updated	2023-02-01 15:48:00 UTC
Description	The crewjam/saml go library prior to version 0.4.9 is vulnerable to an authentication bypass when processing SAML respon

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Merge pull request from GHSA-j2jp-wvqg-wc2g · crewjam/saml@aee3fb1 · GitHub	MISC	github.com	
crewjam/saml Signature Bypass ≈ Packet Storm	MISC	packetstormsecurity.com	
Signature bypass via multiple Assertion elements · Advisory · crewjam/saml · GitHub	CONFIRM	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

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