CVE-2020-12676

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

Summary

CVE	CVE-2020-12676
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-02 20:15:00 UTC
Updated	2021-04-30 17:33:00 UTC
Description	FusionAuth fusionauth-samlv2 0.2.3 allows remote attackers to forge messages and bypass authentication via a SAML ass

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Compass-security	Fusionauth-samlv2	0.2.3	All	All	All
Application	Compass-security	Fusionauth-samlv2	0.2.3	All	All	All
Application	Fusionauth	Samlv2	0.2.3	All	All	All

References

Reference	Source	Link
GitHub - SAMLRaider/SAMLRaider: SAML2 Burp Extension	MISC	github.c
Full Disclosure: CVE-2020-12676 - FusionAuth SAML v2.0 bindings in Java using JAXB - Signature Exclusion Attack	FULLDISC	seclists.
www.nds.ruhr-uni-bochum.de/media/nds/veroeffentlichungen/2012/08/22/BreakingSAML_3.pdf	MISC	www.nd
compass-security.com/fileadmin/Research/Advisories/2020-06_CSNC-2020-002_FusionAut...	MISC	compas
FusionAuth-SAMLv2 0.2.3 Message Forging ≈ Packet Storm	MISC	packetst
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.

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