CVE-2022-35741

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

Summary

CVE	CVE-2022-35741
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-18 15:15:00 UTC
Updated	2022-07-25 17:59:00 UTC
Description	Apache CloudStack version 4.5.0 and later has a SAML 2.0 authentication Service Provider plugin which is found to be vulr

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Cloudstack	All	All	All	All
Application	Apache	Cloudstack	4.17.0.0	All	All	All

References

Reference	Source	Link	Tags
lists.apache.org/thread/hwhxvtwp1d5dsm156bsf1cnyvtmrfv3f	MISC	lists.apache.org	
oss-security - [ADVISORY] Apache CloudStack SAML Single Sign-On XXE (CVE-2022-35741)	MLIST	www.openwall.com	
oss-security - Re: [ADVISORY] Apache CloudStack SAML Single Sign-On XXE (CVE-2022-35741)	MLIST	www.openwall.com	
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

Vendor Comments And Credit

Discovery Credit

LEGACY: This issue was reported by v3ged0ge

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