



CVE-2023-40593

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-40593
State	PUBLIC
Assigner	prodsec@splunk.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-30 17:15:00 UTC
Updated	2023-11-07 04:20:00 UTC
Description	In Splunk Enterprise versions lower than 9.0.6 and 8.2.12, a malicious actor can send a malformed security assertion mark

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Splunk	Splunk	All	All	All	All
Application	Splunk	Splunk Cloud Platform	All	All	All	All

References

Reference	Source	Link	Tags
Splunk DoS Using Malformed SAML Request - Splunk Security Content	MISC	research.splunk.com	
SVD-2023-0802 Splunk Vulnerability Disclosure	MISC	advisory.splunk.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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