CVE-2020-7693

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

Summary

CVE	CVE-2020-7693
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-07-09 14:15:00 UTC
Updated	2022-07-12 17:42:00 UTC
Description	Incorrect handling of Upgrade header with the value websocket leads in crashing of containers hosting sockjs apps. This af

Risk And Classification

Problem Types: CWE-755

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Sour
Call res.write instead of res.end in writeHead by brycekahle · Pull Request #265 · sockjs/sockjs-node · GitHub	MISC
Denial of Service (DoS) in sockjs | Snyk	MISC
Denial of Service (DoS) in org.webjars.npm:sockjs | Snyk	MISC
GitHub - andsnw/sockjs-dos-py: CVE-2020-7693: SockJS 0.3.19 Denial of Service POC	MISC
ERR_STREAM_WRITE_AFTER_END when issuing upgrade request on non-existent URL · Issue #252 · sockjs/sockjs-node · GitHub	MISC
Merge pull request #266 from cakoose/backport-writeHead-fix · sockjs/sockjs-node@dd7e642 · GitHub	MISC
CVE Program record	CVE.
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: Andrew Snow

Legacy QID Mappings

982737 Nodejs (npm) Security Update for sockjs (GHSA-c9g6-9335-x697)