CVE-2020-36048

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-36048
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-08 00:15:00 UTC
Updated	2021-01-12 03:55:00 UTC
Description	Engine.IO before 4.0.0 allows attackers to cause a denial of service (resource consumption) via a POST request to the long

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Socket	Engine.io	All	All	All	All
Application	Socket	Engine.io	All	All	All	All

References

Reference	Source	Link	Tags
SocketIO / EngineIO DoS | callerxyz	MISC	blog.caller.xyz	Exploit, Third Pa
feat: decrease the default value of maxHttpBufferSize · socketio/engine.io@734f9d1 · GitHub	MISC	github.com	Patch, Third Pa
GitHub - bcaller/kill-engine-io: DoS python-engineio / socketio via the long polling transport	MISC	github.com	Third Party Adv
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

No vendor comments have been submitted for this CVE.

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

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