



CVE-2020-36049

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

Summary

CVE	CVE-2020-36049
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-08 00:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	socket.io-parser before 3.4.1 allows attackers to cause a denial of service (memory consumption) via a large packet because

Risk And Classification

Problem Types: CWE-770

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
fix: prevent DoS (OOM) via massive packets (#95) · socketio/socket.io-parser@dcb942d · GitHub	MISC	github.com	Patch, Third Party
SocketIO / EngineIO DoS callerxyz	MISC	blog.caller.xyz	Exploit, Third Party
GitHub - bcaller/kill-engine-io: DoS python-engineio / socketio via the long polling transport	MISC	github.com	Third Party
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, cve

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

982029 Nodejs (npm) Security Update for socket.io-parser (GHSA-xfhh-g9f5-x4m4)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)