



CVE-2017-16031

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

Summary

CVE	CVE-2017-16031
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-04 19:29:00 UTC
Updated	2018-07-31 14:42:00 UTC
Description	Socket.io is a realtime application framework that provides communication via websockets. Because socket.io 0.9.6 and ea

Risk And Classification

Problem Types: CWE-330

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	T
Overview	MISC	nodesecurity.io	T
ID generation vulnerability · Issue #856 · socketio/socket.io · GitHub	MISC	github.com	Is
Making ID generation securely random · socketio/socket.io@67b4eb9 · GitHub	MISC	github.com	Is
Fix for ID generation vulnerability #856 by martinthomson · Pull Request #857 · socketio/socket.io · GitHub	MISC	github.com	Is
CVE Program record	CVE.ORG	www.cve.org	cr
NVD vulnerability detail	NVD	nvd.nist.gov	cr

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980903 Nodejs (npm) Security Update for socket.io (GHSA-qv2v-m59f-v5fw)

© [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](#)