



CVE-2015-9236

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

Summary

CVE	CVE-2015-9236
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-05-31 20:29:00 UTC
Updated	2019-10-09 23:15:00 UTC
Description	Hapi versions less than 11.0.0 implement CORS incorrectly and allowed for configurations that at best returned inconsisten

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hapijs	Hapi	All	All	All	All
Application	Hapijs	Hapi	All	All	All	All

References

Reference	Source	Link	Tags
11.0.0 Release Notes · Issue #2850 · hapijs/hapi · GitHub	MISC	github.com	Relea
CORS route-specific override can conflict with connection defaults · Issue #2840 · hapijs/hapi · GitHub	MISC	github.com	Patch
Node Security Project	MISC	nodesecurity.io	Third
CVE Program record	CVE.ORG	www.cve.org	canor
NVD vulnerability detail	NVD	nvd.nist.gov	canor

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

984056 Nodejs (npm) Security Update for hapi (GHSA-vwrf-r5r4-7775)

© [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](#).

Free CVE JSON API [cve.report/api](#)

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