CVE-2015-9235

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-9235
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-05-29 20:29:00 UTC
Updated	2019-10-09 23:15:00 UTC
Description	In jsonwebtoken node module before 4.2.2 it is possible for an attacker to bypass verification when a token digitally signed

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Auth0	Jsonwebtoken	All	All	All	All
Application	Auth0	Jsonwebtoken	All	All	All	All

References

Reference	Source	Link
Critical vulnerabilities in JSON Web Token libraries	MISC	www.t
Critical vulnerabilities in JSON Web Token libraries	MISC	auth0
Verification with an asymmetric key of a token signed with a symmetri… · auth0/node-jsonwebtoken@1bb584b · GitHub	MISC	github
Overview	MISC	nodes
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

983931 Nodejs (npm) Security Update for jsonwebtoken (GHSA-c7hr-j4mj-j2w6)

© 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 registred 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