



CVE-2016-10555

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

Summary

CVE	CVE-2016-10555
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 23:16:00 UTC
Description	Since "algorithm" isn't enforced in jwt.decode() in jwt-simple 0.3.0 and earlier, a malicious user could choose what algorithm

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jwt-simple Project	Jwt-simple	All	All	All	All

References

Reference
Add an algorithm parameter to the decode method by gregorypratt · Pull Request #16 · hokaccha/node-jwt-simple · GitHub
Critical vulnerabilities in JSON Web Token libraries
Add a verify(token, algorithm, verificationKey) method as per this posting regarding vulnerabilities in jwt: https://auth0.com/blog/2015/03/31/critical-vulnerabilities-in-json-web-token-libraries
Overview
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[983173](#) Nodejs (npm) Security Update for jwt-simple (GHSA-vgrx-w6rg-8fqf)

© [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](#)