



CVE-2019-9153

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

Summary

CVE	CVE-2019-9153
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-08-22 16:15:00 UTC
Updated	2019-08-30 12:52:00 UTC
Description	Improper Verification of a Cryptographic Signature in OpenPGP.js <=4.1.2 allows an attacker to forge signed messages by

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openpgpjs	Openpgpjs	All	All	All	All

References

Reference	Source	Link	Tags
Security fixes by twiss · Pull Request #797 · openpgpjs/openpgpjs · GitHub	CONFIRM	github.com	Patch, Third Party Advisory
OpenPGP.js 4.2.0 Signature Bypass / Invalid Curve Attack ≈ Packet Storm	MISC	packetstormsecurity.com	Third Party Advisory, V
Multiple Vulnerabilities in OpenPGP.js – SEC Consult	MISC	sec-consult.com	Exploit, Third Party Adv
Security fixes by twiss · Pull Request #816 · openpgpjs/openpgpjs · GitHub	CONFIRM	github.com	Third Party Advisory
Release v4.2.0 - Security Release · openpgpjs/openpgpjs · GitHub	CONFIRM	github.com	Release Notes
BSI - Publications - Mailvelope Extensions Security Audit	MISC	www.bsi.bund.de	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[981667](#) Nodejs (npm) Security Update for openpgp (GHSA-qwqc-28w3-fww6)

© [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](#)