



CVE-2019-9155

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

Summary

CVE	CVE-2019-9155
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-08-22 16:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	A cryptographic issue in OpenPGP.js <=4.2.0 allows an attacker who is able provide forged messages and gain feedback a

Risk And Classification

Problem Types: CWE-327

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
Fix ECDH message encryption for some session keys by twiss · Pull Request #853 · openpgpjs/openpgpjs · GitHub	CONFIRM	github.com
Release v4.3.0 - Security Release · openpgpjs/openpgpjs · GitHub	CONFIRM	github.com
OpenPGP.js 4.2.0 Signature Bypass / Invalid Curve Attack ≈ Packet Storm	MISC	packetstor
Multiple Vulnerabilities in OpenPGP.js – SEC Consult	MISC	sec-consu
Fix ECDH message encryption for some session keys by twiss · Pull Request #853 · openpgpjs/openpgpjs · GitHub	CONFIRM	github.com
BSI - Publications - Mailvelope Extensions Security Audit	MISC	www.bsi.b
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.gc

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[981970](#) Nodejs (npm) Security Update for openpgp (GHSA-77jf-fjjf-xcww)

© [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](#)