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.con
Release v4.3.0 - Security Release · openpgpjs/openpgpjs · GitHub	CONFIRM	github.con
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.con
BSI - Publications - Mailvelope Extensions Security Audit	MISC	www.bsi.b
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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