



CVE-2015-8013

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

Summary

CVE	CVE-2015-8013
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-25 18:29:00 UTC
Updated	2017-08-10 13:15:00 UTC
Description	s2k.js in OpenPGP.js will decrypt arbitrary messages regardless of passphrase for crafted PGP keys which allows remote a

Risk And Classification

Problem Types: CWE-310

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
Throw exception on unsupported S2K type. · openpgpjs/openpgpjs@668a9bb · GitHub	CONFIRM	github.com	Patch, Third
Openpgp.js 's2k.js' Predictable Session Key Security Bypass Vulnerability	BID	www.securityfocus.com	Third Party A
oss-security - Re: CVE Request: Openpgp.js Critical vulnerability in S2K	MLIST	www.openwall.com	Mailing List
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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