CVE-2017-11424

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-11424
State	PUBLIC
Assigner	security@duo.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-24 16:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	In PyJWT 1.5.0 and below the `invalid_strings` check in `HMACAlgorithm.prepare_key` does not account for all PEM encoc

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Pyjwt Project	Pyjwt	All	All	All	All

References

Reference	Source	Link	Ta
Guard against PKCS1 PEM-encoded public keys by jpadilla · Pull Request #277 · jpadilla/pyjwt · GitHub	CONFIRM	github.com	Iss
Debian -- Security Information -- DSA-3979-1 pyjwt	DEBIAN	www.debian.org	Thi
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report