



CVE-2021-41117

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

Summary

CVE	CVE-2021-41117
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-10-11 17:15:00 UTC
Updated	2021-10-19 02:19:00 UTC
Description	keypair is a a RSA PEM key generator written in javascript. keypair implements a lot of cryptographic primitives on its own c

Risk And Classification

Problem Types: CWE-335

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Keypair Project	Keypair	All	All	All	All

References

Reference	Source	Link	Tags
GitHub Security Lab Securing the world's software, together	MISC	securitylab.github.com	
Insecure random number generation · Advisory · juliangruber/keypair · GitHub	CONFIRM	github.com	
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

980403 Nodejs (npm) Security Update for keypair (GHSA-3f99-hvg4-qjwj)

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