



CVE-2021-29245

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

Summary

CVE	CVE-2021-29245
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-05 13:15:00 UTC
Updated	2021-05-11 13:50:00 UTC
Description	BTCPay Server through 1.0.7.0 uses a weak method Next to produce pseudo-random values to generate a legacy API key

Risk And Classification

Problem Types: CWE-338

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Btcpayserver	Btcpay Server	All	All	All	All
Application	Btcpayserver	Btcpay Server	All	All	All	All

References

Reference	Source	Link	Tags
Vulnerability Disclosure affecting BTCPay Server	MISC	blog.btcpayserver.org	
Releases · btcpayserver/btcpayserver · GitHub	MISC	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.

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

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