



CVE-2021-3908

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

Summary

CVE	CVE-2021-3908
State	PUBLIC
Assigner	cna@cloudflare.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-11-11 22:15:00 UTC
Updated	2022-08-09 13:42:00 UTC
Description	OctoRPKI does not limit the depth of a certificate chain, allowing for a CA to create children in an ad-hoc fashion, thereby r

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cloudflare	Octorpm	All	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All

References

Reference	Source	Link	Tag
Infinite certificate chain depth results in OctoRPKI running forever · Advisory · cloudflare/cfrpm · GitHub	MISC	github.com	
Debian -- Security Information -- DSA-5041-1 cfrpm	DEBIAN	www.debian.org	
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

Vendor Comments And Credit

Discovery Credit

LEGACY: Koen van Hove

Legacy QID Mappings

178993 Debian Security Update for cfrpm (DSA 5041-1)

101700 Debian Security Update for cfrpm (DSA 5041-1) CVE-2021-3908

184/62 Debian Security Update for ctrpki (CVE-2021-3908)

980107 Go (go) Security Update for github.com/cloudflare/cfrpki/cmd/octorpci (GHSA-g5gj-9ggf-9vmq)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)