



# CVE-2021-3911

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

## Summary

<b>CVE</b>	CVE-2021-3911
<b>State</b>	PUBLIC
<b>Assigner</b>	cna@cloudflare.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-11-11 22:15:00 UTC
<b>Updated</b>	2022-04-04 14:03:00 UTC
<b>Description</b>	If the ROA that a repository returns contains too many bits for the IP address then OctoRPKI will crash.

## Risk And Classification

**Problem Types:** CWE-252

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Cloudflare</a>	<a href="#">Octorpm</a>	All	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All

## References

Reference	Source	Link	Tags
Misconfigured IP address field in ROA leads to OctoRPKI crash · Advisory · cloudflare/cfrpm · GitHub	MISC	<a href="#">github.com</a>	
Debian -- Security Information -- DSA-5041-1 cfrpm	DEBIAN	<a href="#">www.debian.org</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** Koen van Hove

## Legacy QID Mappings

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

184229 Debian Security Update for cfrpm (CVE-2021-3911)

© [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](#)