



CVE-2020-17366

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

Summary

CVE	CVE-2020-17366
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-08-05 22:15:00 UTC
Updated	2023-01-27 21:01:00 UTC
Description	An issue was discovered in NLnet Labs Routinator 0.1.0 through 0.7.1. It allows remote attackers to bypass intended access

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ninetlabs	Routinator	All	All	All	All

References

Reference	Source	Link
Missing files don't result in a Manifest/PP being considered invalid · Issue #319 · NLnetLabs/routinator · GitHub	MISC	github.com
Release 0.8.0 'Strikes and Gutters, Ups and Downs' · NLnetLabs/routinator · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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](#)