CVE-2020-5420

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-5420
State	PUBLIC
Assigner	security@pivotal.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-03 01:15:00 UTC
Updated	2020-09-11 15:42:00 UTC
Description	Cloud Foundry Routing (Gorouter) versions prior to 0.206.0 allow a malicious developer with "cf push" access to cause den

Risk And Classification

Problem Types: CWE-754

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cloudfoundry	Cf-deployment	All	All	All	All
Application	Cloudfoundry	Cf-deployment	All	All	All	All
Application	Cloudfoundry	Gorouter	All	All	All	All
Application	Cloudfoundry	Gorouter	All	All	All	All

References

Reference	Source	Link	Ta
CVE-2020-5420: Gorouter is vulnerable to DoS attack via invalid HTTP responses | Cloud Foundry	CONFIRM	www.cloudfoundry.org	V
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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

CVE.report and Source URL Uptime Status status.cve.report