



CVE-2020-5401

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

Summary

CVE	CVE-2020-5401
State	PUBLIC
Assigner	security@pivotal.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-27 20:15:00 UTC
Updated	2020-03-03 19:43:00 UTC
Description	Cloud Foundry Routing Release, versions prior to 0.197.0, contains GoRouter, which allows malicious clients to send invalid

Risk And Classification

Problem Types: CWE-444

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cloudfoundry	Routing Release	All	All	All	All
Application	Cloudfoundry	Routing Release	All	All	All	All

References

Reference	Source	Link	Tags
CVE-2020-5401: Cloud Foundry GoRouter is vulnerable to cache poisoning Cloud Foundry	CONFIRM	www.cloudfoundry.org	Vendor
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

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](#)