



CVE-2020-5423

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

Summary

CVE	CVE-2020-5423
State	PUBLIC
Assigner	security@pivotal.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-02 02:15:00 UTC
Updated	2020-12-04 18:39:00 UTC
Description	CAPI (Cloud Controller) versions prior to 1.101.0 are vulnerable to a denial-of-service attack in which an unauthenticated m

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
CVE-2020-5423: Cloud Controller is vulnerable to denial of service via YAML parsing Cloud Foundry	CONFIRM	www.cloudfoundry.org
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.

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](#)