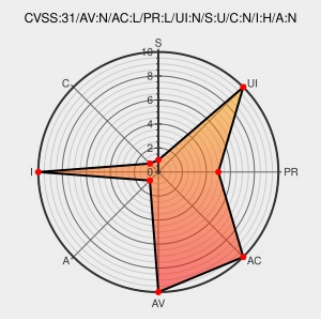
CVE-2017-14389

Published on: 11/28/2017 12:00:00 AM UTC

Last Modified on: 05/25/2021 07:34:00 PM UTC

CVE-2017-14389

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Capi-release from Cloudfoundry contain the following vulnerability:

An issue was discovered in Cloud Foundry Foundation capi-release (all versions prior to 1.45.0), cf-release (all versions prior to v280), and cf-deployment (all versions prior to v1.0.0). The Cloud Controller does not prevent space developers from creating subdomains to an already existing route that belongs to a different user in a different org and space, aka an "Application Subdomain Takeover."

CVE-2017-14389 has been assigned by security_alert@emc.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
CVE-2017-14389: Application Subdomain Takeover via Cloud Foundry Private Domains | Cloud Foundry	Issue Tracking, Third Party Advisory	CONFIRM www.cloudfoundry.org/cve-2017-

www.cloudfoundry.org 14389/
text/html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:cloudfoundry:capi-release:*:*:*:*:*:*:*:*:

cpe:2.3:a:cloudfoundry:cf-deployment:*:*:*:*:*:*:*:*:

cpe:2.3:a:cloudfoundry:cf-release:*:*:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:capi-release:*:*:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:capi-release:*:*:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:cf-deployment:*:*:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:cf-deployment:*:*:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:cf-release:*:*:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:cf-release:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID Next ID→

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