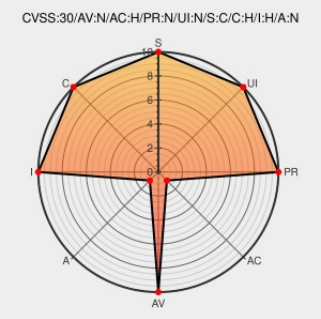
CVE-2019-3788

Published on: 04/25/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:43 PM UTC

CVE-2019-3788

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



Certain versions of Uaa Release from Cloudfoundry contain the following vulnerability:

Cloud Foundry UAA Release, versions prior to 71.0, allows clients to be configured with an insecure redirect uri. Given a UAA client was configured with a wildcard in the redirect uri's subdomain, a remote malicious unauthenticated user can craft a phishing link to get a UAA access code from the victim.

CVE-2019-3788 has been assigned by security_alert@emc.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Cloud Foundry** - **UAA Release (OSS)** version **v71.0**

Affected Vendor/Software: **Pivotal** - **Pivotal Application Service** version **2.5.1**

CVSS3 Score: 6.1 - MEDIUM

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

CVSS2 Score: 5.8 - MEDIUM

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

CVE References

Description	Tags	Link

Description	Tags	Link
CVE-2019-3788: UAA redirect-uri allows wildcard in the subdomain | Cloud Foundry	Vendor Advisory www.cloudfoundry.org text/html	CONFIRM www.cloudfoundry.org/blog/cve-2019-3788

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:cloudfoundry:uaa_release:*:*:*:*:*:*:*:*:

cpe:2.3:a:cloudfoundry:uaa_release:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→