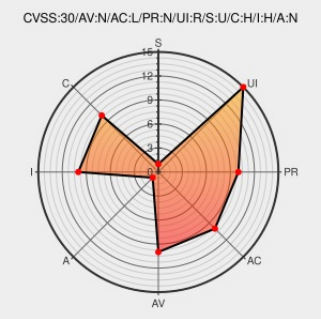
CVE-2019-3793

Published on: 04/24/2019 12:00:00 AM UTC

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

CVE-2019-3793

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



Certain versions of Application Service from Pivotal Software contain the following vulnerability:

Pivotal Apps Manager Release, versions 665.0.x prior to 665.0.28, versions 666.0.x prior to 666.0.21, versions 667.0.x prior to 667.0.7, contain an invitation service that accepts HTTP. A remote unauthenticated user could listen to network traffic and gain access to the authorization credentials used to make the invitation requests.

CVE-2019-3793 has been assigned by security_alert@emc.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Pivotal** - **Apps Manager** version **666.0.21**

Affected Vendor/Software: **Pivotal** - **Apps Manager** version **667.0.7**

Affected Vendor/Software: **Pivotal** - **Apps Manager** version **665.0.28**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
CVE-2019-3793: Invitations Service supports HTTP connections | Security | VMware Tanzu	Vendor Advisory pivotal.io text/html	CONFIRM pivotal.io/security/cve-2019-3793

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	Pivotal Software	Application Service	All	All	All	All
Application	Pivotal Software	Application Service	All	All	All	All

cpe:2.3:a:pivotal_software:application_service:*:*:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:application_service:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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