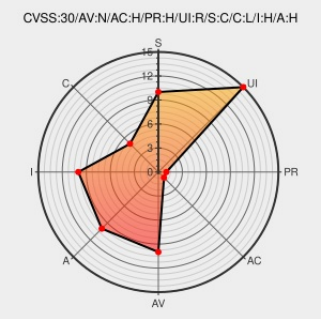
CVE-2020-5425

Published on: 10/31/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:03 PM UTC

CVE-2020-5425

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



Certain versions of Single Sign-on For Tanzu from Vmware contain the following vulnerability:

Single Sign-On for Vmware Tanzu all versions prior to 1.11.3 ,1.12.x versions prior to 1.12.4 and 1.13.x prior to 1.13.1 are vulnerable to user impersonation attack.If two users are logged in to the SSO operator dashboard at the same time, with the same username, from two different identity providers, one can acquire the token of the other and thus operate with their permissions. Note: Foundation may be vulnerable only if: 1) The system zone is set up to use a SAML identity provider 2) There are internal users that have the same username as users in the external SAML provider 3) Those duplicate-named users have the scope to access the SSO operator dashboard 4) The vulnerability doesn't appear with LDAP because of chained authentication.

CVE-2020-5425 has been assigned by security@pivotal.io to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **VMware Tanzu** - **Single Sign-On for VMware Tanzu** version **< 1.11.3**

Affected Vendor/Software: **VMware Tanzu** - **Single Sign-On for VMware Tanzu** version **< 1.12.4**

Affected Vendor/Software: **VMware Tanzu** - **Single Sign-On for VMware Tanzu** version **< 1.13.1**

CVSS3 Score: 7.9 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	HIGH	HIGH

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication

NETWORK	HIGH	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
CVE-2020-5425: User Impersonation possible in Tanzu SSO | Security | VMware Tanzu	Vendor Advisory tanzu.vmware.com text/html	CONFIRM tanzu.vmware.com/security/cve-2020-5425

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vmware	Single Sign-on For Tanzu	All	All	All	All
Application	Vmware	Single Sign-on For Tanzu	All	All	All	All

cpe:2.3:a:vmware:single_sign-on_for_tanzu:*:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:single_sign-on_for_tanzu:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→