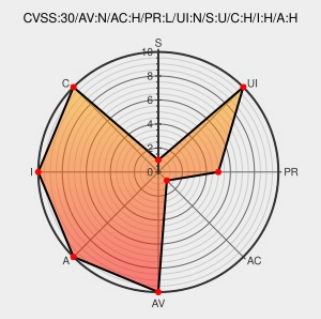
CVE-2017-2297

Published on: 02/01/2018 12:00:00 AM UTC

Last Modified on: 01/24/2022 04:46:00 PM UTC

CVE-2017-2297

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



Certain versions of Puppet from Puppet contain the following vulnerability:

Puppet Enterprise versions prior to 2016.4.5 and 2017.2.1 did not correctly authenticate users before returning labeled RBAC access tokens. This issue has been fixed in Puppet Enterprise 2016.4.5 and 2017.2.1. This only affects users with labeled tokens, which is not the default for tokens.

CVE-2017-2297 has been assigned by security@puppet.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Puppet** - **Puppet Enterprise** version **2016.4.x prior to 2016.4.5, 2016.5.x, 2017.1.x**

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 6 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
CVE-2017-2297 - Incorrect Credential Management with Labeled RBAC	Vendor Advisory	CONFIRM

Tokens | Puppet.com

puppet.com
text/html

puppet.com/security/cve/cve-2017-2297

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	Puppet	Puppet	All	All	All	All
Application	Puppet	Puppet	2016.5.1	All	All	All
Application	Puppet	Puppet	2016.5.2	All	All	All
Application	Puppet	Puppet	2017.1.0	All	All	All
Application	Puppet	Puppet	2017.1.1	All	All	All
Application	Puppet	Puppet	All	All	All	All
Application	Puppet	Puppet	2016.5.1	All	All	All
Application	Puppet	Puppet	2016.5.2	All	All	All
Application	Puppet	Puppet	2017.1.0	All	All	All
Application	Puppet	Puppet	2017.1.1	All	All	All
Application	Puppet	Puppet Enterprise	All	All	All	All
Application	Puppet	Puppet Enterprise	2016.5.1	All	All	All
Application	Puppet	Puppet Enterprise	2016.5.2	All	All	All
Application	Puppet	Puppet Enterprise	2017.1.0	All	All	All
Application	Puppet	Puppet Enterprise	2017.1.1	All	All	All

cpe:2.3:a:puppet:puppet:*:*:*:*:enterprise:*:*:*:

cpe:2.3:a:puppet:puppet:2016.5.1:*:*:*:enterprise:*:*:*:

cpe:2.3:a:puppet:puppet:2016.5.2:*:*:*:enterprise:*:*:*:

cpe:2.3:a:puppet:puppet:2017.1.0:*:*:*:enterprise:*:*:*:

cpe:2.3:a:puppet:puppet:2017.1.1:*:*:*:enterprise:*:*:*:

cpe:2.3:a:puppet:puppet:*:*:*:*:enterprise:*:*:*:

cpe:2.3:a:puppet:puppet:2016.5.1:*:*:*:enterprise:*:*:*:

cpe:2.3:a:puppet:puppet:2016.5.2:*:*:*:enterprise:*:*:*:

cpe:2.3:a:puppet:puppet:2017.1.0:*:*:*:enterprise:*:*:*:

cpe:2.3:a:puppet:puppet:2017.1.1:*:*:*:enterprise:*:*:*:

cpe:2.3:a:puppet:puppet_enterprise:*:*:*:*:*:*:*:*:

cpe:2.3:a:puppet:puppet_enterprise:2016.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:puppet:puppet_enterprise:2016.5.2:*:*:*:*:*:*:*:

cpe:2.3:a:puppet:puppet_enterprise:2017.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:puppet:puppet_enterprise:2017.1.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→