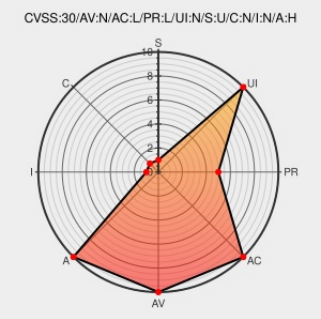
CVE-2017-2296

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

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

CVE-2017-2296

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



Certain versions of Puppet from Puppet contain the following vulnerability:

In Puppet Enterprise 2017.1.x and 2017.2.1, using specially formatted strings with certain formatting characters as Classifier node group names or RBAC role display names causes errors, effectively causing a DOS to the service. This was resolved in Puppet Enterprise 2017.2.2.

CVE-2017-2296 has been assigned by security@puppet.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Puppet** - **Puppet Enterprise** version **2017.1.x, 2017.2.1. Fixed in 2017.2.2**

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	NONE	HIGH

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
CVE-2017-2296 - RBAC and Classifier errors caused by specially crafted strings | Puppet	Vendor Advisory puppet.com text/html	CONFIRM puppet.com/security/cve/cve-2017-2296

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	2017.1.0	All	All	All
Application	Puppet	Puppet	2017.1.1	All	All	All
Application	Puppet	Puppet	2017.2.1	All	All	All
Application	Puppet	Puppet	2017.1.0	All	All	All
Application	Puppet	Puppet	2017.1.1	All	All	All
Application	Puppet	Puppet	2017.2.1	All	All	All
Application	Puppet	Puppet Enterprise	2017.1.0	All	All	All
Application	Puppet	Puppet Enterprise	2017.1.1	All	All	All
Application	Puppet	Puppet Enterprise	2017.2.1	All	All	All

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:2017.2.1:*:*:*: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:2017.2.1:*:*:*:enterprise:*:*:*:

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

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

cpe:2.3:a:puppet:puppet_enterprise:2017.2.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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