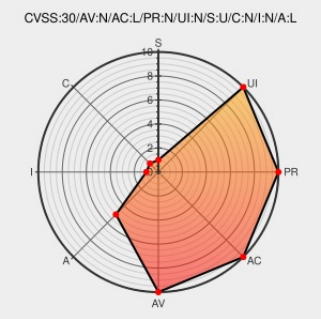
CVE-2016-9686

Published on: 02/08/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:16 PM UTC

CVE-2016-9686

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



Certain versions of Puppet Enterprise from Puppet contain the following vulnerability:

The Puppet Communications Protocol (PCP) Broker incorrectly validates message header sizes. An attacker could use this to crash the PCP Broker, preventing commands from being sent to agents. This is resolved in Puppet Enterprise 2016.4.3 and 2016.5.2.

CVE-2016-9686 has been assigned by security@puppet.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Puppet** - **Puppet Enterprise** version **2015.3.x**

Affected Vendor/Software: **Puppet** - **Puppet Enterprise** version **2016.x prior to 2016.4.3**

Affected Vendor/Software: **Puppet** - **Puppet Enterprise** version **2016.5.1.**

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
CVE-2016-9686 - Denial of Service in Puppet Communications Protocol Broker | Puppet	Vendor Advisory puppet.com text/html	CONFIRM puppet.com/security/cve/cve-2016-9686

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 Enterprise	All	All	All	All
Application	Puppet	Puppet Enterprise	2016.5.1	All	All	All
Application	Puppet	Puppet Enterprise	All	All	All	All
Application	Puppet	Puppet Enterprise	2016.5.1	All	All	All

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

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→