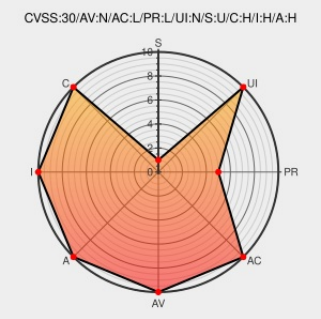
CVE-2015-7330

Published on: 04/11/2016 12:00:00 AM UTC

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

CVE-2015-7330

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



Certain versions of Puppet from Puppet contain the following vulnerability:

Puppet Enterprise 2015.3 before 2015.3.1 allows remote attackers to bypass a host whitelist protection mechanism by leveraging the Puppet communications protocol.

CVE-2015-7330 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

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

CVE References

Description	Tags	Link
Puppet Enterprise Configuration Error Lets Remote Non-Whitelisted Users Access the Target System - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1034550

CVE-2015-7330 | Puppet Labs

Vendor Advisory
puppetlabs.com
text/html

CONFIRM
puppetlabs.com/security/cve/cve-2015-7330

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	2015.3.0	All	All	All
Application	Puppet	Puppet	2015.3.0	All	All	All
Application	Puppet	Puppet Enterprise	2015.3.0	All	All	All

cpe:2.3:a:puppet:puppet:2015.3.0:*:*:*:enterprise:*:*:*:

cpe:2.3:a:puppet:puppet:2015.3.0:*:*:*:enterprise:*:*:*:

cpe:2.3:a:puppet:puppet_enterprise:2015.3.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→