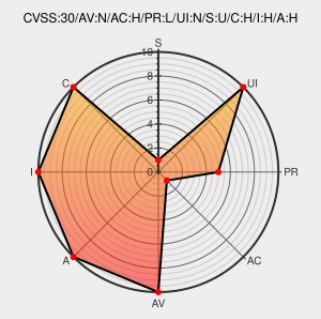
CVE-2016-9599

Published on: 04/23/2018 12:00:00 AM UTC

Last Modified on: 08/04/2021 05:15:00 PM UTC

CVE-2016-9599

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



Certain versions of Puppet-tripleo from Openstack contain the following vulnerability:

puppet-tripleo before versions 5.5.0, 6.2.0 is vulnerable to an access-control flaw in the IPtables rules management, which allowed the creation of TCP/UDP rules with empty port values. If SSL is enabled, a malicious user could use these open ports to gain access to unauthorized resources.

CVE-2016-9599 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

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
1409687 – (CVE-2016-9599) CVE-2016-9599 puppet-tripleo: if ssl is enabled, traffic is open on both undercloud and overcloud	Issue Tracking Third Party Advisory bugzilla.redhat.com	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2016-9599

	text/html	
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2017:0025

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	Openstack	Puppet-tripleo	5.5.0	All	All	All
Application	Openstack	Puppet-tripleo	6.2.0	All	All	All
Application	Openstack	Puppet-tripleo	5.5.0	All	All	All
Application	Openstack	Puppet-tripleo	6.2.0	All	All	All
Application	Redhat	Openstack	10	All	All	All
Application	Redhat	Openstack	10.0	All	All	All
Application	Redhat	Openstack	10.0	All	All	All

cpe:2.3:a:openstack:puppet-tripleo:5.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:puppet-tripleo:6.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:puppet-tripleo:5.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:puppet-tripleo:6.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:10:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:10.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:10.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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