

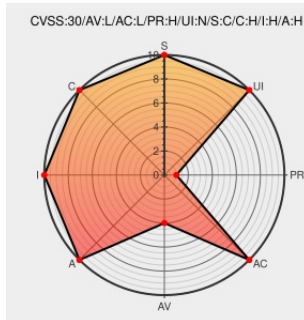


CVE-2017-2627

Published on: 08/22/2018 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:12:05 PM UTC

CVE-2017-2627

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Tripleo-common](#) from [Openstack](#) contain the following vulnerability:

A flaw was found in openstack-tripleo-common as shipped with Red Hat Openstack Enterprise 10 and 11. The sudoers file as installed with OSP's openstack-tripleo-common package is much too permissive. It contains several lines for the mistral user that have wildcards that allow directory traversal with '..' and it grants full passwordless root access to the validations user.

CVE-2017-2627 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Red Hat - openstack-tripleo-common** version = **As shipped with Red Hat Openstack Enterprise 10 and 11**

CVSS3 Score: **8.2 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	HIGH	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.2 - HIGH**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
-------------	------	------

Description

1421917 – (CVE-2017-2627) CVE-2017-2627 openstack-tripleo-common: sudoers file is too permissive

Tags

Issue Tracking

Vendor Advisory

bugzilla.redhat.com

text/html

Link

CONFIRM

bugzilla.redhat.com/show_bug.cgi?id=CVE-2017-2627

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	Tripleo-common	-	All	All	All
Application	Openstack	Tripleo-common	-	All	All	All
Application	Redhat	Openstack	10	All	All	All
Application	Redhat	Openstack	10.0	All	All	All
Application	Redhat	Openstack	11	All	All	All
Application	Redhat	Openstack	11.0	All	All	All
Application	Redhat	Openstack	10.0	All	All	All
Application	Redhat	Openstack	11.0	All	All	All

cpe:2.3:a:openstack:tripleo-common:-:*:*:*:*:*:

cpe:2.3:a:openstack:tripleo-common:-:*:*:*:*:*:

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

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

cpe:2.3:a:redhat:openstack:11:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:11.0:*:*:*:*:*:

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

cpe:2.3:a:redhat:openstack:11.0:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)