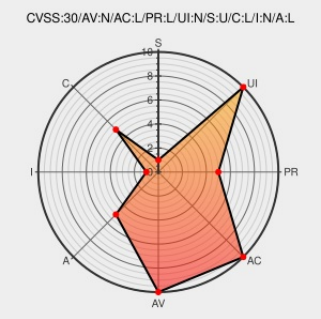
CVE-2015-5295

Published on: 01/20/2016 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:53:00 AM UTC

CVE-2015-5295

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



Certain versions of Fedora from Fedoraproject contain the following vulnerability:

The template-validate command in OpenStack Orchestration API (Heat) before 2015.1.3 (kilo) and 5.0.x before 5.0.1 (liberty) allows remote authenticated users to cause a denial of service (memory consumption) or determine the existence of local files via the resource type in a template, as demonstrated by file:///dev/zero.

CVE-2015-5295 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.4 - MEDIUM

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

CVSS2 Score: 5.5 - MEDIUM

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

CVE References

Description	Tags	Link
Oracle Solaris Bulletin - April 2016	Third Party Advisory www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/bulletinapr2016-2952098.html

Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2016:0442
OpenStack Heat CVE-2015-5295 Denial of Service Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 81438
Bug #1496277 "[OSSA 2016-003] template-validate may read server ..." : Bugs : OpenStack Heat	Patch Third Party Advisory bugs.launchpad.net text/html	CONFIRM bugs.launchpad.net/heat/+bug/1496277
CVE-2015-5295 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2015-5295
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2016:0440
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2016:0441
Bug 1298295 – CVE-2015-5295 openstack-heat: Vulnerability in Heat template validation leading to DoS	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1298295
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:0266
OSSA-2016-003: Heat denial of service through template-validate — OpenStack Security Advisories 2014.2.0.dev100 documentation	Vendor Advisory security.openstack.org text/html	CONFIRM security.openstack.org/ossa/OSSA-2016-003.html
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2016:0266
[SECURITY] Fedora 23 Update: openstack-heat-2015.1.2-2.fc23	Mailing List Third Party Advisory lists.fedoraproject.org text/html	FEDORA FEDORA-2016-fe5b9da308

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Application	Openstack	Orchestration Api	All	All	All	All
Application	Openstack	Orchestration Api	All	All	All	All

Operating System	Oracle	Solaris	11.3	All	All	All
Operating System	Oracle	Solaris	11.3	All	All	All
Application	Redhat	Openstack	7.0	All	All	All
Application	Redhat	Openstack	7.0	All	All	All

- cpe:2.3:o:fedoraproject:fedora:23:*:*:*:*:*:*:*:
- cpe:2.3:o:fedoraproject:fedora:23:*:*:*:*:*:*:*:
- cpe:2.3:a:openstack:orchestration_api:*:*:*:*:*:*:*:*:
- cpe:2.3:a:openstack:orchestration_api:*:*:*:*:*:*:*:*:
- cpe:2.3:o:oracle:solaris:11.3:*:*:*:*:*:*:*:
- cpe:2.3:o:oracle:solaris:11.3:*:*:*:*:*:*:*:
- cpe:2.3:a:redhat:openstack:7.0:*:*:*:*:*:*:*:
- cpe:2.3:a:redhat:openstack:7.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→