



CVE-2013-6426

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2013-6426
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-12-14 17:21:00 UTC
Updated	2017-08-29 01:33:00 UTC
Description	The cloudformation-compatible API in OpenStack Orchestration API (Heat) before Havana 2013.2.1 and Icehouse before ic

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openstack	Heat	All	All	All	All

References

Reference	Source	Link	Tags
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
oss-security - [OSSA 2013-034] Heat CFN policy rules not all enforced (CVE-2013-6426)	MLIST	www.openwall.com	
Red Hat Customer Portal	REDHAT	rhn.redhat.com	
OpenStack Heat CFN Policy CVE-2013-6426 Security Bypass Vulnerability	BID	www.securityfocus.com	
Bug #1256049 "[OSSA 2013-034] Heat CFN policy rules not all info..." : Bugs : heat	CONFIRM	bugs.launchpad.net	Exp
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#)