



CVE-2012-2094

Published on: 06/05/2012 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:24 AM UTC

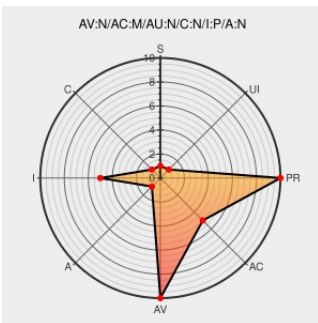
CVE-2012-2094

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Horizon](#) from [Openstack](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in the refresh mechanism in the log viewer in horizon/static/horizon/js/horizon.js in OpenStack Dashboard (Horizon) folsom-1 and 2012.1 and earlier allows remote attackers to inject arbitrary web script or HTML via the guest console.

CVE-2012-2094 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

PARTIAL

NONE

CVE References

Description

Tags

Link

Bug #977944 "refreshing in log viewer interprets html and javasc..." : Bugs : OpenStack Dashboard (Horizon)

bugs.launchpad.net
[text/html](#)

[MISC bugs.launchpad.net/horizon/+bug/977944](https://bugs.launchpad.net/horizon/+bug/977944)

[SECURITY] Fedora 17 Update: python-django-horizon-2012.1-2.fc17

lists.fedoraproject.org
[text/html](#)

[FEDORA FEDORA-2012-6108](#)

Security Advisory SA49024 - OpenStack Dashboard (Horizon) Session Fixation and Script Insertion Vulnerabilities - Secunia

[Vendor Advisory](#)
web.archive.org
[text/html](#)

[SECUNIA 49024](#)

IBM X-Force Exchange

exchange.xforce.ibmcloud.com

[XF openstack-horizon-xss\(76136\)](#)

exchange.openstack.org	text/html	OpenStack Horizon XSS (CVE-2012-0417)
Security Advisory SA49071 - Ubuntu update for horizon - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 49071
[OSSA 2012-004] XSS vulnerability in Horizon log viewer : Mailing list archive : openstack team in Launchpad	lists.launchpad.net text/html	MLIST [openstack] 20120417 [OSSA 2012-004] XSS vulnerability in Horizon viewer
USN-1439-1: Horizon vulnerabilities Ubuntu	ubuntu.com text/html	UBUNTU USN-1439-1
html escape the console log in refresh · openstack/horizon@7f8c788 · GitHub	github.com text/html	CONFIRM github.com/openstack/horizon/commit/7f8c788aa70db98ac904f37fa4197fcabb8
No Description Provided	www.osvdb.org	OSVDB 81742
Inactive Link Not Archived		

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	Horizon	2012.1	All	All	All
Application	Openstack	Horizon	folsom-1	All	All	All
Application	Openstack	Horizon	2012.1	All	All	All
Application	Openstack	Horizon	folsom-1	All	All	All
cpe:2.3:a:openstack:horizon:2012.1:*.***:***:*						
cpe:2.3:a:openstack:horizon:folsom-1:*.***:***:*						
cpe:2.3:a:openstack:horizon:2012.1:*.***:***:*						
cpe:2.3:a:openstack:horizon:folsom-1:*.***:***:*						

No vendor comments have been submitted for this CVE

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](#)