



CVE-2019-3889

Published on: 07/11/2019 12:00:00 AM UTC

Last Modified on: 03/01/2023 04:33:00 PM UTC

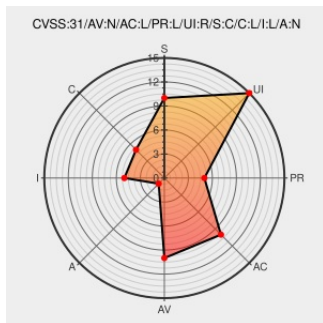
CVE-2019-3889

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [OpenShift Container Platform](#) from [Redhat](#) contain the following vulnerability:

A reflected XSS vulnerability exists in authorization flow of OpenShift Container Platform versions: openshift-online-3, openshift-enterprise-3.4 through 3.7 and openshift-enterprise-3.9 through 3.11. An attacker could use this flaw to steal authorization data by getting them to click on a malicious link.

CVE-2019-3889 has been assigned by [secalert@redhat.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Red Hat** - **atomic-openshift** version = **openshift-online-3, openshift-enterprise-3.4 through 3.7 and openshift-enterprise-3.9 through 3.11**

CVSS3 Score: **5.4 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **3.5 - LOW**

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

CVE References

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

1693499 – (CVE-2019-3889) CVE-2019-3889 atomic-openshift: reflected XSS in authentication flow	bugzilla.redhat.com text/html	 MISC bugzilla.redhat.com/show_bug.cgi?id=1693499
1693499 – (CVE-2019-3889) CVE-2019-3889 atomic-openshift: reflected XSS in authentication flow	Issue Tracking Vendor Advisory bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3889
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2019:3722
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2019:3770
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	 MISC access.redhat.com/errata/RHSA-2020:0795
Red Hat Customer Portal	access.redhat.com text/html	 MISC access.redhat.com/security/cve/CVE-2019-3889

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	Redhat	Openshift Container Platform	4.1	All	All	All
Application	Redhat	Openshift Container Platform	4.2	All	All	All
Application	Redhat	Openshift Container Platform	All	All	All	All
Application	Redhat	Openshift Container Platform	All	All	All	All
cpe:2.3:a:redhat:openshift_container_platform:4.1:*****:*						
cpe:2.3:a:redhat:openshift_container_platform:4.2:*****:*						
cpe:2.3:a:redhat:openshift_container_platform:*****:*						
cpe:2.3:a:redhat:openshift_container_platform:*****:*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)