

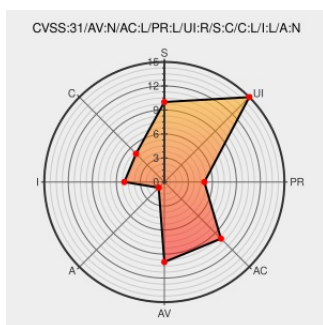


CVE-2021-3442

Published on: Not Yet Published

Last Modified on: 02/12/2023 11:41:00 PM UTC

CVE-2021-3442

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

Certain versions of [Openshift Api Management](#) from [Redhat](#) contain the following vulnerability:

A flaw was found in the Red Hat OpenShift API Management product. User input is not validated allowing an authenticated user to inject scripts into some text boxes leading to a XSS attack. The highest threat from this vulnerability is to data confidentiality.

CVE-2021-3442 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	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVE References

Description	Tags	Link
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2021-3442
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2021:3851
1930083 – (CVE-2021-3442) CVE-2021-3442 PT RHOAM: XSS in 3scale at various places	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1930083

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

Exploit/POC from Github

A flaw was found in the Red Hat OpenShift API Management product. User input is not validated allowing an authenticat...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Openshift Api Management	2.9.1	All	All	All
cpe:2.3:a:redhat:openshift_api_management:2.9.1:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-3442 : A flaw was found in the Red Hat OpenShift API Management product. User input is not validated allow... twitter.com/i/web/status/1...	2022-08-22 15:14:41
 @threatmeter	CVE-2021-3442 A flaw was found in the Red Hat OpenShift API Management product. User input is not validated allowin... twitter.com/i/web/status/1...	2022-08-23 07:09:33
 @ColorTokensInc	Emerging Vulnerability Found CVE-2021-3442 - A flaw was found in the Red Hat OpenShift API Management product. User... twitter.com/i/web/status/1...	2022-08-23 18:12:17
 /r/netcve	CVE-2021-3442	2022-08-22 15:38:34

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#)