

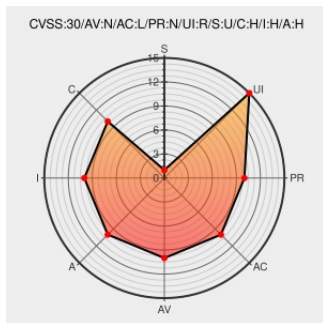


CVE-2018-10899

Published on: 08/01/2019 12:00:00 AM UTC

Last Modified on: 08/04/2021 05:14:00 PM UTC

CVE-2018-10899

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

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

A flaw was found in Jolokia versions from 1.2 to before 1.6.1. Affected versions are vulnerable to a system-wide CSRF. This holds true for properly configured instances with strict checking for origin and referrer headers. This could result in a Remote Code Execution attack.

CVE-2018-10899 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [jolokia](#) - [jolokia](#) version 1.6.1

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
Jolokia – Jolokia	Release Notes Vendor Advisory jolokia.org	CONFIRM jolokia.org/changes-report.html#a1.6.1

	jolokia.org text/html	
Pony Mail!	lists.apache.org text/html	 MLIST [activemq-issues] 20200122 [jira] [Updated] (AMQ-7373) jolokia-core-1.6.0.jar is vulnerable to CVE-2018-10899
1601037 – (CVE-2018-10899) CVE-2018-10899 jolokia: system-wide CSRF that could lead to Remote Code Execution	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-10899
Pony Mail!	lists.apache.org text/html	 MLIST [activemq-issues] 20200122 [jira] [Commented] (AMQ-7373) jolokia-core-1.6.0.jar is vulnerable to CVE-2018-10899
Pony Mail!	lists.apache.org text/html	 MLIST [activemq-issues] 20200122 [jira] [Assigned] (AMQ-7373) jolokia-core-1.6.0.jar is vulnerable to CVE-2018-10899
Pony Mail!	lists.apache.org text/html	 MLIST [activemq-issues] 20200120 [jira] [Work logged] (AMQ-7373) jolokia-core-1.6.0.jar is vulnerable to CVE-2018-10899
Pony Mail!	lists.apache.org text/html	 MLIST [activemq-issues] 20200102 [jira] [Created] (AMQ-7373) jolokia-core-1.6.0.jar is vulnerable to CVE-2018-10899
Pony Mail!	lists.apache.org text/html	 MLIST [activemq-issues] 20200122 [jira] [Work logged] (AMQ-7373) jolokia-core-1.6.0.jar is vulnerable to CVE-2018-10899
Pony Mail!	lists.apache.org text/html	 MLIST [activemq-issues] 20200122 [jira] [Resolved] (AMQ-7373) jolokia-core-1.6.0.jar is vulnerable to CVE-2018-10899
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	 REDHAT RHSA-2019:2413
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2019:2804
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	Jolokia	Jolokia	All	All	All	All
Application	Jolokia	Jolokia	All	All	All	All
Application	Redhat	Openstack	13	All	All	All
Application	Redhat	Openstack	13.0	All	All	All
Application	Redhat	Openstack	13.0	All	All	All

cpe:2.3:a:jolokia:jolokia:*****:

cpe:2.3:a:openstack:openstack:13.0:*:*:*:*:*:
cpe:2.3:a:openstack:openstack:13.0:*:*:*:*:*:
cpe:2.3:a:redhat:openstack:13:*:*:*:*:*:
cpe:2.3:a:redhat:openstack:13.0:*:*:*:*:*:
cpe:2.3:a:redhat:openstack:13.0:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← 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