

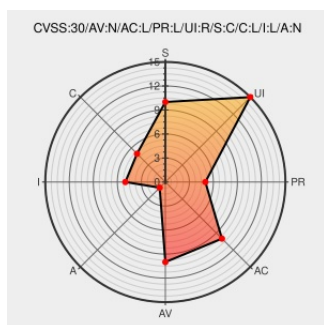


CVE-2018-8024

Published on: 07/12/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:41 PM UTC

CVE-2018-8024

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

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

In Apache Spark 2.1.0 to 2.1.2, 2.2.0 to 2.2.1, and 2.3.0, it's possible for a malicious user to construct a URL pointing to a Spark cluster's UI's job and stage info pages, and if a user can be tricked into accessing the URL, can be used to cause script to execute and expose information from the user's view of the Spark UI. While some browsers

like recent versions of Chrome and Safari are able to block this type of attack, current versions of Firefox (and possibly others) do not.

CVE-2018-8024 has been assigned by security@apache.org to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Apache Software Foundation - Apache Spark** version **1.0.0 to 2.1.2**

Affected Vendor/Software: **Apache Software Foundation - Apache Spark** version **2.2.0 to 2.2.1**

Affected Vendor/Software: **Apache Software Foundation - Apache Spark** version **2.3.0**

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: **4.9 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact

CVE References

Description	Tags	Link
Security Apache Spark	Mitigation Vendor Advisory spark.apache.org text/html	 CONFIRM spark.apache.org/security.html#CVE-2018-8024
Apache Mail Archives	Mailing List Mitigation Vendor Advisory lists.apache.org text/html	 MLIST [dev] 20180711 CVE-2018-8024 Apache Spark XSS vulnerability in UI

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.

Related QID Numbers

[981203](#) Java (maven) Security Update for org.apache.spark:spark-core_2.11 (GHSA-8cw6-5qyp-q3wj)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Spark	2.3.0	All	All	All
Application	Apache	Spark	2.3.0	All	All	All
Application	Apache	Spark	All	All	All	All
Application	Apache	Spark	All	All	All	All
Application	Mozilla	Firefox	-	All	All	All
Application	Mozilla	Firefox	-	All	All	All

cpe:2.3:a:apache:spark:2.3.0:*:*:*:*:*:

cpe:2.3:a:apache:spark:2.3.0:*:*:*:*:*:

cpe:2.3:a:apache:spark:*:*:*:*:*:

cpe:2.3:a:apache:spark:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:*:*:*:*:*:

No vendor comments have been submitted for this CVE

© [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](#)