

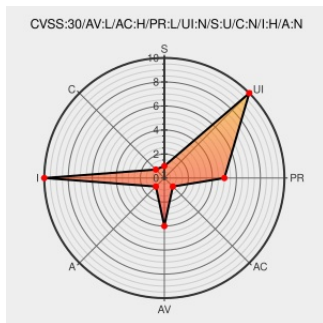


CVE-2018-1334

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

Last Modified on: 03/23/2021 11:24:31 PM UTC

CVE-2018-1334

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

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

In Apache Spark 1.0.0 to 2.1.2, 2.2.0 to 2.2.1, and 2.3.0, when using PySpark or SparkR, it's possible for a different local user to connect to the Spark application and impersonate the user running the Spark application.

CVE-2018-1334 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: **4.7 - MEDIUM**

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

CVSS2 Score: **1.9 - LOW**

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

CVE References

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.

[981255](#) Java (maven) Security Update for org.apache.spark:spark-core_2.11 (GHSA-6mqg-8r44-vmjc)

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
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:*****:.*:						

← Previous ID

Next ID→