



CVE-2023-25504

Published on: Not Yet Published

Last Modified on: 04/27/2023 02:08:00 PM UTC

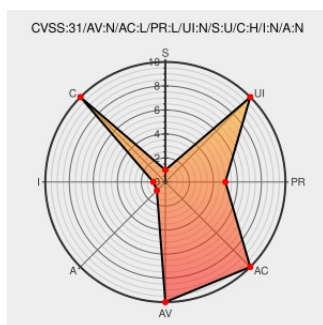
CVE-2023-25504

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

A malicious actor who has been authenticated and granted specific permissions in Apache Superset may use the import dataset feature in order to conduct Server-Side Request Forgery attacks and query internal resources on behalf of the server where Superset is deployed. This vulnerability exists in Apache Superset versions up to and

including 2.0.1.

CVE-2023-25504 has been assigned by security@apache.org to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Apache Software Foundation - Apache Superset** version <= 2.0.1

CVSS3 Score: **6.5 - MEDIUM**

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

CVE References

Description	Tags	Link
oss-security - Re: CVE-2023-25504: Apache Superset: Possible SSRF on import datasets	www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2023/04/18/8
No Description Provided	lists.apache.org text/html	MISC lists.apache.org/thread/tdnzkocfsqg2sbbornnp9g492fn4zhtx

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	Apache	Superset	All	All	All	All
cpe:2.3:a:apache:superset:*****.*.*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2023-25504 : A malicious actor who has been authenticated and granted specific permissions in #Apache Superset... twitter.com/i/web/status/1...	2023-04-17 17:03:20
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2023-25504 A malicious actor who has been authenticated and granted specific... twitter.com/i/web/status/1...	2023-04-17 18:11:00

[← 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](#)