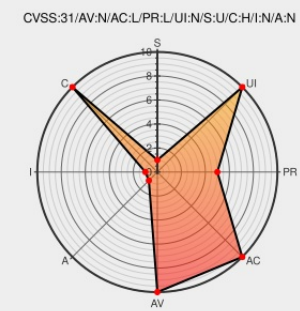
CVE-2023-30776

Published on: Not Yet Published

Last Modified on: 06/15/2023 08:15:00 AM UTC

CVE-2023-30776

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Superset from Apache contain the following vulnerability:

An authenticated user with specific data permissions could access database connections stored passwords by requesting a specific REST API. This issue affects Apache Superset version 1.3.0 up to 2.0.1.

CVE-2023-30776 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
No Description Provided	lists.apache.org text/html	MISC lists.apache.org/thread/s9w9w10mt2sngk3solwnmq5k7md53tsz
oss-security - CVE-2023-30776: Apache Superset: Database connection password leak	www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2023/04/24/3

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-2023-30776 : An authenticated user with specific data permissions could access database connections stored pass… twitter.com/i/web/status/1…	2023-04-24 16:06:25
@oss_security	CVE-2023-30776: Apache Superset: Database connection password leak: Posted by Daniel Gaspar on Apr 24Description:… twitter.com/i/web/status/1…	2023-04-24 16:30:36

← Previous ID

Next ID→