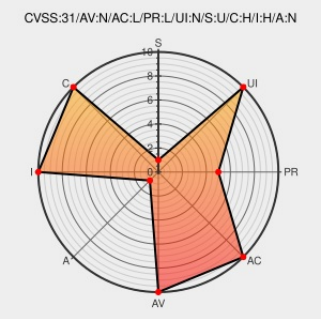
CVE-2020-13952

Published on: 09/30/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:42 PM UTC

CVE-2020-13952

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



Certain versions of Superset from Apache contain the following vulnerability:

In the course of work on the open source project it was discovered that authenticated users running queries against Hive and Presto database engines could access information via a number of templated fields including the contents of query description metadata database, the hashed version of the authenticated users' password, and access to connection information including the plaintext password for the current connection. It would also be possible to run arbitrary methods on the database connection object for the Presto or Hive connection, allowing the user to bypass security controls internal to Superset. This vulnerability is present in every Apache Superset version < 0.37.2.

CVE-2020-13952 has been assigned by security@apache.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.1 - HIGH

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

CVSS2 Score: 5.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	MISC lists.apache.org/thread.html/rf1faa368f580d2cb691576bee1277855f769667f3114d5df1dacbea6%40%3Cdev

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

982694 Python (pip) Security Update for apache-superset (GHSA-77pw-c3j2-5fc8)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Superset	All	All	All	All
Application	Apache	Superset	All	All	All	All

cpe:2.3:a:apache:superset:*:*:*:*:*:*:*:*:

cpe:2.3:a:apache:superset:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→