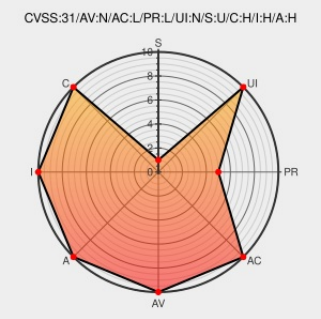
CVE-2020-13948

Published on: 09/17/2020 12:00:00 AM UTC

Last Modified on: 11/21/2022 01:55:00 PM UTC

CVE-2020-13948

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



Certain versions of Superset from Apache contain the following vulnerability:

While investigating a bug report on Apache Superset, it was determined that an authenticated user could craft requests via a number of templated text fields in the product that would allow arbitrary access to Python's `os` package in the web application process in versions < 0.37.1. It was thus possible for an authenticated user to list and access files, environment variables, and process information. Additionally it was possible to set environment variables for the current process, create and update files in folders writable by the web process, and execute arbitrary programs accessible by the web process. All other operations available to the `os` package in Python were also available, even if not explicitly enumerated in this CVE.

CVE-2020-13948 has been assigned by security@apache.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Pony Mail!	lists.apache.org text/html	MLIST [superset-notifications] 20201112 [GitHub] [incubator-superset] ktmud commented on pull request 'chevron' library for templating as jinja alternative
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	MISC lists.apache.org/thread.html/rdeee068ac1e0c43bd5b69830240f30598df15a2ef9f7998c7b29131e%40%3Cde
Pony Mail!	lists.apache.org text/html	MLIST [superset-notifications] 20201112 [GitHub] [incubator-superset] robdiciuccio commented on pull re support 'chevron' library for templating as jinja alternative

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
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

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→