

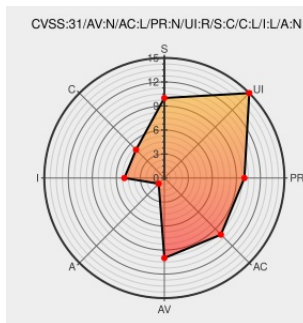


CVE-2021-28125

Published on: 04/27/2021 12:00:00 AM UTC

Last Modified on: 05/07/2021 05:57:00 PM UTC

CVE-2021-28125

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

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

Apache Superset up to and including 1.0.1 allowed for the creation of an external URL that could be malicious. By not checking user input for open redirects the URL shortener functionality would allow for a malicious user to create a short URL for a dashboard that could convince the user to click the link.

CVE-2021-28125 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 <= 1.0.1

Vulnerability Patch/Work Around

<https://github.com/apache/superset/pull/13461>

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **5.8 - MEDIUM**

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

CVE References

Description	Tags	Link
Pony Mail!	lists.apache.org text/html	 MLIST [superset-dev] 20210427 CVE-2021-28125: Apache Superset Open Redirect
oss-security - CVE-2021-28125: Apache Superset Open Redirect	www.openwall.com text/html	 MLIST [oss-security] 20210427 CVE-2021-28125: Apache Superset Open Redirect

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

980513 Python (pip) Security Update for superset (GHSA-pfwg-rxf4-97c3)

Exploit/POC from Github

PoC for exploiting CVE-2021-28125

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Superset	All	All	All	All
<code>cpe:2.3:a:apache:superset:*.***.*.*.*.*:</code>						

Discovery Credit

Found and reported by Gianluca Veltri, Dario Castrogiovanni

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-28125 : #Apache Superset up to and including 1.0.1 allowed for the creation of an external URL that could... twitter.com/i/web/status/1...	2021-04-27 09:30:27
 /r/netcve	CVE-2021-28125	2021-04-27 09:41:20

[← Previous ID](#)

Next ID→

[site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report