



CVE-2021-27907

Published on: 03/05/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:49 PM UTC

CVE-2021-27907

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

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

Apache Superset up to and including 0.38.0 allowed the creation of a Markdown component on a Dashboard page for describing chart's related information. Abusing this functionality, a malicious user could inject javascript code executing unwanted action in the context of the user's browser. The javascript code will be automatically executed

(Stored XSS) when a legitimate user surfs on the dashboard page. The vulnerability is exploitable creating a “div” section and embedding in it a “svg” element with javascript code.

CVE-2021-27907 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 <= 0.38.0

CVSS3 Score: **5.4 - MEDIUM**

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

CVSS2 Score: **3.5 - LOW**

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

CVE References

Description	Tags	Link				
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [superset-dev] 20210305 CVE-2021-27907: Apache Superset stored XSS on Dashboard markdown				
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:*:*:*:*:*:						
Discovery Credit						
This issue was reported by Gianluca Veltri and Dario Castrogiovanni of Cuebiq						
← Previous ID			Next ID →			