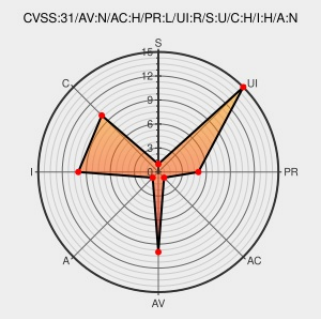
CVE-2021-41172

Published on: 10/26/2021 12:00:00 AM UTC

Last Modified on: 10/27/2021 08:27:00 PM UTC

CVE-2021-41172 - advisory for GHSA-j8j6-f829-w425

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



Certain versions of Antsword Redis from Antsword Redis Project contain the following vulnerability:

AS_Redis is an AntSword plugin for Redis. The Redis Manage plugin for AntSword prior to version 0.5 is vulnerable to Self-XSS due to due to insufficient input validation and sanitization via redis server configuration. Self-XSS in the plugin configuration leads to code execution. This issue is patched in version 0.5.

CVE-2021-41172 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Medicean** - **AS_Redis** version **< 0.5**

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

v0.4 Self-XSS in host addr · Issue #1 · AntSword-Store/AS_Redis · GitHub	github.com text/html	MISC github.com/AntSword-Store/AS_Redis/issues/1
从虚假的XSS到放弃RCE再到Self-RCE	mp.weixin.qq.com text/html	MISC mp.weixin.qq.com/s/yjuG6DLT_bSRnpggPj21Xw
Self-XSS in AS_Redis · Advisory · Medicean/AS_Redis · GitHub	github.com text/html	CONFIRM github.com/Medicean/AS_Redis/security/advisories/GHSA-j8j6-f829-w425

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	Antsword Redis Project	Antsword Redis	All	All	All	All

cpe:2.3:a:antsword_redis_project:antsword_redis:*:*:*:*:*:antsword:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-41172 : AS_Redis is an AntSword plugin for Redis. The Redis Manage plugin for AntSword prior to version 0.… twitter.com/i/web/status/1…	2021-10-26 14:09:54

← Previous ID

Next ID→