

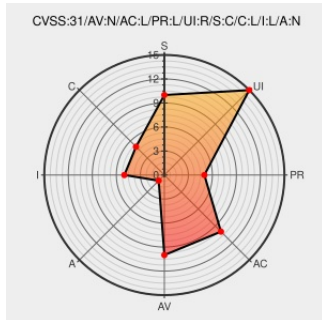


CVE-2022-3024

Published on: Not Yet Published

Last Modified on: 12/09/2022 07:39:00 PM UTC

CVE-2022-3024

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

Certain versions of [Simple Bitcoin Faucets](#) from [Simple Bitcoin Faucets Project](#) contain the following vulnerability:

The Simple Bitcoin Faucets WordPress plugin through 1.7.0 does not have any authorisation and CSRF in an AJAX action, allowing any authenticated users, such as subscribers to call it and add/delete/edit Bonds. Furthermore, due to the lack of sanitisation and escaping, it could also lead to Stored Cross-Site Scripting issues

CVE-2022-3024 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Unknown - Bitcoin Satoshi Tools : Faucets, Visitor Rewarder, Satoshi Games, Referral Program** version **<= 1.7.0**

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

CVE References

Description	Tags	Link
Simple Bitcoin Faucets <= 1.7.0 - Unauthorised AJAX Call to Stored XSS WordPress Security Vulnerability	web.archive.org text/html Inactive Link Not Archived	MISC wpscan.com/vulnerability/7f43cb8e-0c1b-4528-8c5c-b81ab42778dc

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

Exploit/POC from Github

```
cve update exploit poc rce sqli code cve-2022-3024 Log4j jndi rmi
`mysql://root:123djnes71dsaasj@mysql.tencent.com` 辣...
```

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Simple Bitcoin Faucets Project	Simple Bitcoin Faucets	All	All	All	All
cpe:2.3:a:simple_bitcoin_faucets_project:simple_bitcoin_faucets:*:*:*:*:wordpress:*:*:						

Discovery Credit

Lana Codes

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-3024 : The Simple Bitcoin Faucets WordPress plugin through 1.7.0 does not have any authorisation and CSRF... twitter.com/i/web/status/1...	2022-09-26 12:42:02
 @LinInfoSec	Wordpress - CVE-2022-3024: wpscan.com/vulnerability/...	2022-09-26 16:00:32
 @phpadvisories	CVE-2022-3024 Simple Bitcoin Faucets Plugin up to 1.7.0 on WordPress AJAX Action cross site scripting zpr.io/tpw2iRBhsCcP #phpsec	2022-09-26 17:24:53
 /r/netcve	CVE-2022-3024	2022-09-26 13:39:01

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)