

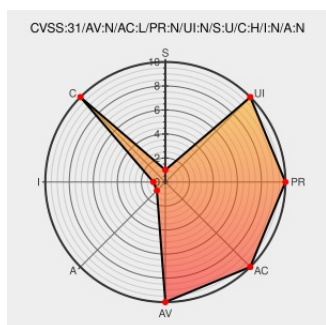


CVE-2021-37491

Published on: Not Yet Published

Last Modified on: 02/15/2023 04:49:00 PM UTC

CVE-2021-37491

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

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

An issue discovered in src/wallet/wallet.cpp in Dogecoin Project Dogecoin Core 1.14.3 and earlier allows attackers to view sensitive information via CWallet::CreateTransaction() function.

CVE-2021-37491 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
Dogecoin	dogecoin.com text/html	MISC dogecoin.com
BlkVulnReport/NDSS23_BlockScope.pdf at main · VPRLab/BlkVulnReport · GitHub	github.com text/html	MISC github.com/VPRLab/BlkVulnReport/blob/main/NDSS23_BlockScope.pdf
[vulnerability] Possible privacy leakage due to ordered transaction inputs · Issue #2279 · dogecoin/dogecoin · GitHub	github.com text/html	MISC github.com/dogecoin/dogecoin/issues/2279
shuffle selected coins before transaction finalization · bitcoin/bitcoin@2fb9c1e · GitHub	github.com text/html	MISC github.com/bitcoin/bitcoin/commit/2fb9c1e6681370478e24a19172ed6d78d95d50c
dogecoin/wallet.cpp at master · dogecoin/dogecoin · GitHub	github.com text/html	MISC github.com/dogecoin/dogecoin/blob/master/src/wallet/wallet.cpp#L2628-L2640

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

An issue discovered in src/wallet/wallet.cpp in Dogecoin Project Dogecoin Core 1.14.3 and earlier allows attackers to...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dogecoin	Dogecoin	All	All	All	All
cpe:2.3:a:dogecoin:dogecoin:*:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-37491 : An issue discovered in src/wallet/wallet.cpp in Dogecoin Project Dogecoin Core 1.14.3 and earlier... twitter.com/i/web/status/1...	2023-02-07 14:06:44
 @threatmeter	CVE-2021-37491 An issue discovered in src/wallet/wallet.cpp in Dogecoin Project Dogecoin Core 1.14.3 and earlier al... twitter.com/i/web/status/1...	2023-02-07 23:22:06
 @JohnJasonFallow	New vulnerability on the NVD: CVE-2021-37491 ift.tt/sxJ0d4p	2023-02-09 06:11:08
 @doogsineerg	New vulnerability on the NVD: CVE-2021-37491 ift.tt/bR7T8pS	2023-02-09 06:33:39
 @xanadulinux	CVE-2021-37491 ift.tt/kuryECh	2023-02-09 06:52:13
 @geekphane	#CyberSecurity #Security #CERT #CVE #Nist #breach #vulnerability : CVE-2021-37491	2023-02-12 07:55:12
 /r/netcve	CVE-2021-37491	2023-02-07 14:39:25

← Previous ID

Next ID →

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](#)