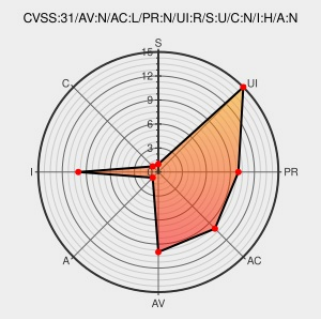
CVE-2020-17753

Published on: 06/24/2021 12:00:00 AM UTC

Last Modified on: 07/01/2021 01:22:00 PM UTC

CVE-2020-17753

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



Certain versions of Rcpro from Rcpro Project contain the following vulnerability:

An issue was discovered in function addMeByRC in the smart contract implementation for RC, an Ethereum token, allows attackers to transfer an arbitrary amount of tokens to an arbitrary address.

CVE-2020-17753 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Attention Required! | Cloudflare	etherscan.io, text/html, Inactive Link, Not Archived	MISC etherscan.io/address/0x403E518F21F5Ce308085Dcf6637758C61f92446A
blockchains/Phishing.md at	github.com	MISC github.com/hellowuzekai/blockchains/blob/master/Phishing.md

master · hellowuzekai/blockchains · GitHub	text/html	
Attention Required! | Cloudflare	etherscan.io text/html Inactive Link Not Archived	MISC etherscan.io/address/0x86b784AEF0e9c9A581550bA07fb85B64c780c320
Attention Required! | Cloudflare	etherscan.io text/html Inactive Link Not Archived	MISC etherscan.io/address/0x07c1C8c2BCe6290DAA554118b7d208041615CE54
Attention Required! | Cloudflare	etherscan.io text/html Inactive Link Not Archived	MISC etherscan.io/address/0x340DbA127F099DAB9DC8599C75b16e44D9b02Fdb
Attention Required! | Cloudflare	etherscan.io text/html Inactive Link Not Archived	MISC etherscan.io/address/0xD7aA007C3e7ab454FFE3E20F0b28F926Db295477
Attention Required! | Cloudflare	etherscan.io text/html Inactive Link Not Archived	MISC etherscan.io/address/0x5a50C7D96fC68ea2F0bEE06D86CD971c31F85604

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	Rcpro Project	Rcpro	-	All	All	All
Application	Rc Project	Rc	-	All	All	All

cpe:2.3:a:rcpro_project:rcpro:-:*:*:*:*:*:*:*:

cpe:2.3:a:rc_project:rc:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2020-17753 : An issue was discovered in function addMeByRC in the smart contract implementation for RC, an Ethe… twitter.com/i/web/status/1…	2021-06-24 20:06:47
@0_exploit	CVE-2020-17753 dlvr.it/S2QW7P	2021-06-25 05:59:04
/r/netcve	CVE-2020-17753	2021-06-24 20:41:52

← 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 registred 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