



CVE-2021-32684

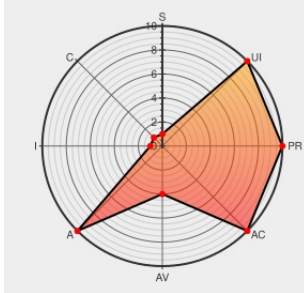
Published on: 06/14/2021 12:00:00 AM UTC

Last Modified on: 06/29/2021 03:36:00 PM UTC

CVE-2021-32684 - advisory for GHSA-52qp-gwwh-qrg4

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

CVSS:31/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H



Certain versions of [Magento-scripts](#) from [Scandipwa](#) contain the following vulnerability:

magento-scripts contains scripts and configuration used by Create Magento App, a zero-configuration tool-chain which allows one to deploy Magento 2. In versions 1.5.1 and 1.5.2, after changing the function from synchronous to asynchronous there wasn't implemented handler in the start, stop, exec, and logs commands, effectively making them unusable. Version 1.5.3 contains patches for the problems.

CVE-2021-32684 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: scandipwa - create-magento-app version $\geq 1.5.1$, $\leq 1.5.2$

CVSS3 Score: **5.5 - MEDIUM**

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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
-------------	------	------

Description	Tags	Link
Missing Handler in @scandipwa/magento-scripts · Advisory · scandipwa/create-magento-app · GitHub	github.com text/html	 CONFIRM github.com/scandipwa/create-magento-app/security/advisories/GHSA-52qp-gwwh-qrg4
fixed exec and logs command throwing an error with docker.getContainers · scandipwa/create-magento-app@89115db · GitHub	github.com text/html	 MISC github.com/scandipwa/create-magento-app/commit/89115db7031e181eb8fb4ec2822bc6cab88e7071

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.

Related QID Numbers

982089 Nodejs (npm) Security Update for @scandipwa/magento-scripts (GHSA-52qp-gwwh-qrg4)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Scandipwa	Magento-scripts	1.5.1	All	All	All
Application	Scandipwa	Magento-scripts	1.5.2	All	All	All
cpe:2.3:a:scandipwa:magento-scripts:1.5.1:*:*:*:*:node.js:*:*						
cpe:2.3:a:scandipwa:magento-scripts:1.5.2:*:*:*:*:node.js:*:*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-32684 : magento-scripts contains scripts and configuration used by Create Magento App, a zero-configuratio... twitter.com/i/web/status/1...	2021-06-14 23:06:56
 /r/netcve	CVE-2021-32684	2021-06-14 23:41:28

[← 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](#)