



CVE-2021-23420

Published on: 08/11/2021 12:00:00 AM UTC

Last Modified on: 08/19/2021 07:42:00 PM UTC

CVE-2021-23420

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

S:S:31/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L/E:F/RL:O/R



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

This affects the package codeception/codeception from 4.0.0 and before 4.1.22, before 3.1.3. The RunProcess class can be leveraged as a gadget to run arbitrary commands on a system that is deserializing user input without validation.

CVE-2021-23420 has been assigned by report@snyk.io to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **10 - HIGH**

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

CVE References

Description	Tags	Link
GitHub - JinYiTong/poc	github.com text/html	MISC github.com/JinYiTong/poc
Security: Disable deserialization of RunProcess class by Naktibalda · Pull Request #6241 ·	github.com text/html	MISC github.com/Codeception/Codeception/pull/6241

Codeception/Codeception · GitHub

Deserialization of Untrusted Data in codeception/codeception | Snyk

snyk.io
text/html

MISC snyk.io/vuln/SNYK-PHP-CODECEPTIONCODECEPTION-1324585

Codeception/RunProcess.php at 4.1 · Codeception/Codeception · GitHub

github.com
text/html

MISC github.com/Codeception/Codeception/blob/4.1/ext/RunProcess.php%23L52

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	Codeception	Codeception	All	All	All	All

cpe:2.3:a:codeception:codeception:*****:

Discovery Credit

JinYiTong

Social Mentions

Source	Title	Posted (UTC)
📧 @CVEreport	CVE-2021-23420 : This affects the package codeception/codeception from 4.0.0 and before 4.1.22, before 3.1.3. The... twitter.com/i/web/status/1...	2021-08-11 12:19:51

← Previous ID

Next ID →