



CVE-2023-28115

Published on: Not Yet Published

Last Modified on: 03/24/2023 04:40:00 PM UTC

CVE-2023-28115 - advisory for GHSA-gq6w-q6wh-jggc

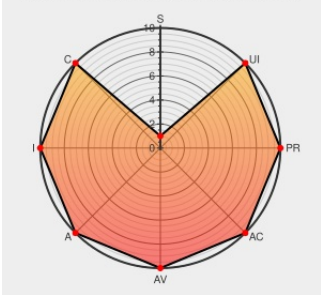
[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)

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



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

Snappy is a PHP library allowing thumbnail, snapshot or PDF generation from a url or a html page. Prior to version 1.4.2, Snappy is vulnerable to PHAR deserialization due to a lack of checking on the protocol before passing it into the `file_exists()` function. If an attacker can upload files of any type to the server he can pass in the `phar://`

protocol to unserialize the uploaded file and instantiate arbitrary PHP objects. This can lead to remote code execution especially when snappy is used with frameworks with documented POP chains like Laravel/Symfony vulnerable developer code. If a user can control the output file from the `generateFromHtml()` function, it will invoke deserialization. This vulnerability is capable of remote code execution if Snappy is used with frameworks or developer code with vulnerable POP chains. It has been fixed in version 1.4.2.

CVE-2023-28115 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **Knplabs** - **snappy** version = < 1.4.2

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

CVE References

Description	Tags	Link
fix: security issue GHSA-gq6w-q6wh-jggc · Knplabs/snappy@1ee6360 · GitHub	github.com text/html	MISC github.com/Knplabs/snappy/commit/1ee6360c9dbbea5d09705909

- Merge pull request #469 from KnpLabs/fix/GHSA-gq6w-q6wh-jggc · KnpLabs/snappy@b66f793 · GitHub
 - [github.com](#)
 - [text/html](#)
 - MISC github.com/KnpLabs/snappy/commit/b66f79334421c26d9c244427
- snappy/AbstractGenerator.php at 5126fb5b335ec929a226314d40cd8dad497c3d67 · KnpLabs/snappy · GitHub
 - [github.com](#)
 - [text/html](#)
 - MISC github.com/KnpLabs/snappy/blob/5126fb5b335ec929a226314d40cd8dad49
- PHAR deserialization allowing remote code execution · Advisory · KnpLabs/snappy · GitHub
 - [github.com](#)
 - [text/html](#)
 - MISC github.com/KnpLabs/snappy/security/advisories/GHSA-gq6w-q6wh-jggc
- Release v1.4.2 · KnpLabs/snappy · GitHub
 - [github.com](#)
 - [text/html](#)
 - MISC github.com/KnpLabs/snappy/releases/tag/v1.4.2
- fix: security issue GHSA-gq6w-q6wh-jggc by AntoineLelaisant · Pull Request #469 · KnpLabs/snappy · GitHub
 - [github.com](#)
 - [text/html](#)
 - MISC github.com/KnpLabs/snappy/pull/469

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	Knplabs	Snappy	All	All	All	All
cpe:2.3:a:knplabs:snappy:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-28115 : Snappy is a PHP library allowing thumbnail, snapshot or PDF generation from a url or a html page.... twitter.com/i/web/status/1...	2023-03-17 22:02:33
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2023-28115 Snappy is a PHP library allowing thumbnail, snapshot or PDF gener... twitter.com/i/web/status/1...	2023-03-17 22:56:00
/r/netcve	CVE-2023-28115	2023-03-17 22:38:17

[← Previous ID](#)

[Next ID →](#)

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](#)