



CVE-2022-2529

Published on: Not Yet Published

Last Modified on: 10/04/2022 04:25:00 PM UTC

CVE-2022-2529

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

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

sflow decode package does not employ sufficient packet sanitisation which can lead to a denial of service attack. Attackers can craft malformed packets causing the process to consume large amounts of memory resulting in a denial of service.

CVE-2022-2529 has been assigned by [cna@cloudflare.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Cloudflare](#) - **goflow** version < 3.4.4

Vulnerability Patch/Work Around

Make sure that the goflow collector is not publicly reachable.

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	NONE	NONE	HIGH

CVE References

Description	Tags	Link
Multiple DoS Attack Vectors in sflow packet handling · Advisory · cloudflare/goflow · GitHub	github.com text/html	MISC github.com/cloudflare/goflow/security/advisories/GHSA-9rpw-2h95-666c

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.com](#)

[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	Cloudflare	Goflow	All	All	All	All
cpe:2.3:a:cloudflare:goflow:*****:						

Discovery Credit

Justin Timperio, Chase Hiltz

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-2529 : sflow decode package does not employ sufficient packet sanitisation which can lead to a denial of s... twitter.com/i/web/status/1...	2022-09-30 10:48:06
 /r/netcve	CVE-2022-2529	2022-09-30 11:38:26

[← 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](#)