



CVE-2023-27594

Published on: Not Yet Published

Last Modified on: 03/24/2023 04:33:00 PM UTC

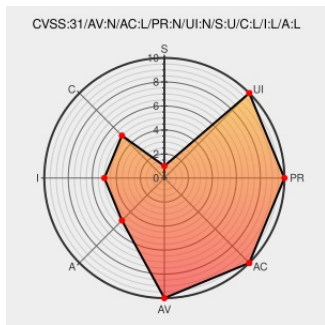
CVE-2023-27594 - advisory for GHSA-8fg8-jh2h-f2hc

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Prior to versions 1.11.15, 1.12.8, and 1.13.1, under specific conditions, Cilium may misattribute the source IP address of traffic to a cluster, identifying external traffic as coming from the host on which Cilium is running. As a consequence, network policies for that cluster might be bypassed, depending on the specific network policies enabled. This issue only manifests when Cilium is routing IPv6 traffic and NodePorts are used to route traffic to pods. IPv6 and endpoint routes are both disabled by default. The problem has been fixed and is available on versions 1.11.15, 1.12.8, and 1.13.1. As a workaround, disable IPv6 routing.

CVE-2023-27594 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [cilium](#) - **cilium** version = < 1.11.15

Affected Vendor/Software: [cilium](#) - **cilium** version = >= 1.12.0, < 1.12.8

Affected Vendor/Software: [cilium](#) - **cilium** version = >= 1.13.0, < 1.13.1

CVSS3 Score: **7.3 - HIGH**

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

CVE References

Description	Tags	Link

Release 1.11.15 · cilium/cilium · GitHub	github.com text/html	MISC github.com/cilium/cilium/releases/tag/v1.11.15
Potential network policy bypass when routing IPv6 traffic · Advisory · cilium/cilium · GitHub	github.com text/html	MISC github.com/cilium/cilium/security/advisories/GHSA-8fg8-jh2h-f2hc
Release 1.13.1 · cilium/cilium · GitHub	github.com text/html	MISC github.com/cilium/cilium/releases/tag/v1.13.1
Release 1.12.8 · cilium/cilium · GitHub	github.com text/html	MISC github.com/cilium/cilium/releases/tag/v1.12.8

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	Cilium	Cilium	All	All	All	All
cpe:2.3:a:cilium:cilium:*:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-27594 : Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Prior t... twitter.com/i/web/status/1...	2023-03-17 20:05:26
/r/netcve	CVE-2023-27594	2023-03-17 20:38:48

[← 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](#)