



# CVE-2023-39347

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2023-39347
<b>State</b>	PUBLIC
<b>Assigner</b>	security-advisories@github.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-09-27 15:18:00 UTC
<b>Updated</b>	2023-09-29 15:54:00 UTC
<b>Description</b>	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. An attacker with the ability to up

## Risk And Classification

**Problem Types:** CWE-345

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Cilium</a>	<a href="#">Cilium</a>	All	All	All	All

## References

Reference	Source	Link	Tags
Threat Model — Cilium 1.15.0-dev documentation	MISC	<a href="https://docs.cilium.io">docs.cilium.io</a>	
Kubernetes users may update Pod labels to bypass network policy · Advisory · cilium/cilium · GitHub	MISC	<a href="https://github.com">github.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[995415](#) GO (Go) Security Update for [github.com/cilium/cilium](https://github.com/cilium/cilium) (GHSA-gj2r-phwg-6rww)

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)