



# CVE-2023-27595

Published on: Not Yet Published

Last Modified on: 03/20/2023 02:46:00 AM UTC

## CVE-2023-27595 - advisory for GHSA-r5x6-w42p-jhpp

[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. In version 1.13.0, when Cilium is started, there is a short period when Cilium eBPF programs are not attached to the host. During this period, the host does not implement any of Cilium's featureset. This can cause disruption to newly established connections during this period due to the lack of Load Balancing, or can cause Network Policy bypass due to the lack of Network Policy enforcement during the window. This vulnerability impacts any Cilium-managed endpoints on the node (such as Kubernetes Pods), as well as the host network namespace (including Host Firewall). This vulnerability is fixed in Cilium 1.13.1 or later. Cilium releases 1.12.x, 1.11.x, and earlier are not affected. There are no known workarounds.

CVE-2023-27595 has been assigned by security-advisories@github.com to track the vulnerability

Affected Vendor/Software: cilium - cilium version == 1.13.0

### CVE References

Description	Tags	Link
Release 1.13.1 · cilium/cilium · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	MISC <a href="https://github.com/cilium/cilium/releases/tag/v1.13.1">github.com/cilium/cilium/releases/tag/v1.13.1</a>
Cilium eBPF filters may be temporarily removed during agent restart · Advisory · cilium/cilium · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	MISC <a href="https://github.com/cilium/cilium/security/advisories/GHSA-r5x6-w42p-jhpp">github.com/cilium/cilium/security/advisories/GHSA-r5x6-w42p-jhpp</a>
bpf.init.sh: make netdev bpf filter cleanup less eager by ti-mo · Pull Request #24336 · cilium/cilium · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	MISC <a href="https://github.com/cilium/cilium/pull/24336">github.com/cilium/cilium/pull/24336</a>

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](mailto: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	<a href="#">Cilium</a>	<a href="#">Cilium</a>	1.13.0	All	All	All
cpe:2.3:a:cilium:cilium:1.13.0:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

### Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2023-27595 : Cilium is a networking, observability, and security solution with an eBPF-based dataplane. In vers... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2023-03-17 22:02:11
 /r/netcve	<a href="#">CVE-2023-27595</a>	2023-03-17 22:38:16

[← 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](#)