CVE-2023-27593

Published on: Not Yet Published

Last Modified on: 03/17/2023 08:15:00 PM UTC

CVE-2023-27593 - advisory for GHSA-4hc4-pgfx-3mrx

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, an attacker with access to a Cilium agent pod can write to `/opt/cni/bin` due to a `hostPath` mount of that directory in the agent pod. By replacing the CNI binary with their own malicious binary and waiting for the creation of a new pod on the node, the attacker can gain access to the underlying node. The issue has been fixed and the fix is available on versions 1.11.15, 1.12.8, and 1.13.1. Some workarounds are available. Kubernetes RBAC should be used to deny users and service accounts `exec` access to Cilium agent pods. In cases where a user requires `exec` access to Cilium agent pods, but should not have access to the underlying node, no workaround is possible.

CVE-2023-27593 has been assigned by security-advisories@github.com to track the vulnerability

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**

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
Using RBAC Authorization | Kubernetes	kubernetes.io text/html	MISC kubernetes.io/docs/reference/access-authn-authz/rbac/
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
agent: install CNI plugin binary in an InitContainer by squeed · Pull Request #24075 · cilium/cilium · GitHub	github.com text/html	MISC github.com/cilium/cilium/pull/24075
cilium-agent container can access the host via `hostPath` mount · Advisory · cilium/cilium · GitHub	github.com	MISC

Advisory · cilium/cilium · GitHub	text/html	github.com/cilium/cilium/security/advisories/GHSA-4hc4-pgfx-3mrx

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 Software

Vendor	Product	Version
Cilium	cilium	= < 1.11.15
Cilium	cilium	= >= 1.12.0, < 1.12.8
Cilium	cilium	= >= 1.13.0, < 1.13.1

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-27593 : Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Prior t… twitter.com/i/web/status/1…	2023-03-17 20:05:03
/r/netcve	CVE-2023-27593	2023-03-17 20:38:47

← Previous ID

Next ID→