Cross-node remote code execution via extension backend BackendData injection

High **thomasferrandiz** published **GHSA-vchx-5pr6-ffx2** 4 days ago

Package

flannel (Kubernetes)

Affected versions

<= v0.28.1

Patched versions

v0.28.2

Description

Background

The Flannel project includes an experimental Extension backend that allows users to easily prototype new backend types.
This backend uses shell commands stored in Kubernetes annotations to configure network connectivity on the node.

Note: you are only affected by this vulnerability if you use the experimental Extension backend. Other backends such as vxlan and wireguard are unaffected.

Vulnerability

This Extension backend is vulnerable to a command injection that allows an attacker who can set Kubernetes Node annotations to achieve root-level arbitrary command execution on every flannel node in the cluster.

The Extension backend's SubnetAddCommand and SubnetRemoveCommand receive attacker-controlled data via stdin (from the `flannel.alpha.coreos.com/backend-data` Node annotation). The content of this annotation is unmarshalled and piped directly to a shell command without checks.

Impact

Kubernetes clusters using Flannel with the Extension backend are affected by this vulnerability. Other backends such as vxlan and wireguard are unaffected.

Patches

This is fixed in version v0.28.2.

Workaround

If you cannot update to a patched version, then use Flannel with another backend such as vxlan or wireguard.

Credits

We would like to thank Shachar Tal from Palo Alto Networks for reporting this vulnerability.

Severity

High 7.5 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	High
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE ID

CVE-2026-32241

Weaknesses

No CWEs

Credits

 **shachartal** Reporter