GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

3 September 2026

Advisory 245: Red Hat Advanced Cluster Management (Submariner) Certificate-Based IPsec Configuration Injection (CVE-2026-66786).

Release Date: 2nd September 2026
Impact: HIGH
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations, System/Network administrators, and Kubernetes/platform engineering teams that deploy or operate Red Hat Advanced Cluster Management (RHACM) for Kubernetes with Submariner multi-cluster networking. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-66786 is a code-injection vulnerability in Submariner, the multi-cluster networking component of Red Hat Advanced Cluster Management (RHACM) for Kubernetes, which connects the networks of separate Kubernetes clusters in a multi-cluster deployment. When Submariner is configured to use certificate-based IPsec authentication mode, its connection configuration is built from free-form strings taken from a Custom Resource Definition (CRD) without proper validation. A malicious or compromised peer cluster in the Submariner mesh can exploit this by publishing a "CableName" value containing newlines and ipsec.conf directives, injecting arbitrary configuration parameters or commands that are executed through Submariner's "leftupdown" hooks - resulting in remote code execution as root on the gateway node.

What are the systems affected?

The following version(s) are affected:

- Red Hat Advanced Cluster Management for Kubernetes deployments running Submariner with certificate-based IPsec authentication mode (IPSecCertAuthMode: true) enabled together with OVN-Kubernetes IPsec – (Affected)

No patched version is currently available. Red Hat's own issue tracker (Bugzilla #2507531) shows this issue remained open (status "NEW"). Red Hat's published guidance is a configuration-based workaround rather than a version upgrade: switch Submariner from certificate-based IPsec authentication mode to the default pre-shared key (PSK) authentication mode by setting IPSecCertAuthMode: false in the SubmarinerConfig custom resource and redeploying the gateway pods. Deployments that do not use certificate-based IPsec authentication mode. The default configuration are not exposed to this specific vulnerability.

What does this mean?

Typical attack flow:

1. **Publish a malicious CableName from a peer cluster in the Submariner mesh**
    - A malicious or compromised peer cluster within a Submariner multi-cluster deployment that has certificate-based IPsec authentication mode enabled publishes a CableName value containing newlines and ipsec.conf directives, which is incorporated into another cluster's gateway configuration without proper validation.
2. **Achieve remote code execution as root on the gateway node**
    - The injected configuration is executed through Submariner's "leftupdown" hooks on the receiving cluster's gateway node, allowing the attacker to run arbitrary commands as root on that node.

Attack vectors:

- Requires membership or compromise of a peer cluster already connected within a Submariner multi-cluster mesh that has both certificate-based IPsec authentication mode and OVN-Kubernetes IPsec enabled (CVSS PR:H) — this is not exploitable by an anonymous external attacker with no foothold in the mesh.
- No user interaction is required (CVSS UI:N) once an attacker controls a malicious or compromised peer cluster. CERTVU is not aware of any report of active exploitation at the time of writing, and the two required non-default configurations mean many RHACM deployments are not exposed at all — but where both settings are enabled, the resulting impact (root code execution on a gateway node) is severe.

Successful exploitation may allow attackers to:

- Execute arbitrary operating-system commands as root on a Submariner gateway node, without needing to authenticate to that node directly.
- Use the compromised gateway node as a foothold into the wider Kubernetes cluster it belongs to, and potentially into every other cluster connected through the same Submariner multi-cluster mesh, since gateway nodes sit at the network boundary between federated clusters.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor workaround without delay, since no patch is currently available

    - If Submariner certificate-based IPsec authentication mode is enabled, switch to the default pre-shared key (PSK) authentication mode by setting IPSecCertAuthMode: false in the SubmarinerConfig custom resource and redeploying the affected gateway pods (per Red Hat's own published mitigation guidance for CVE-2026-66786).

2. Monitor Red Hat's CVE page and Bugzilla #2507531 for a permanent fix, and contact Red Hat Support to confirm the latest guidance for your deployment
3. Audit the estate for RHACM/Submariner deployments using certificate-based IPsec authentication
4. Review Submariner cluster membership and trust boundaries
5. Review gateway node integrity on any deployment that had both prerequisite settings enabled

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-66786
2. https://access.redhat.com/security/cve/CVE-2026-66786