

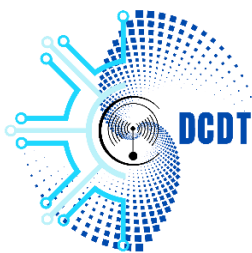
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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

10 September 2026

Advisory 293: Perforce Akana API Platform Policy Manager Authentication Bypass Leading to Unauthenticated Code Injection (CVE-2026-85978).

Release Date: 9th September 2026

Impact: **CRITICAL**

TLP: CLEAR

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

This alert is relevant to Organizations and System/Network administrators that operate Perforce Akana, an enterprise API management platform. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-85978 is a critical vulnerability in the Policy Manager console of Perforce Akana, an enterprise API management platform (API gateway, developer portal, and analytics) used by organizations to publish, secure, and manage their APIs. Perforce is a well-established global enterprise software vendor, and Akana is a widely-deployed enterprise-grade API management product in the same tier as other enterprise DevOps/API infrastructure platforms already judged relevant this session (e.g. JFrog Artifactory, Advisory 240).

What are the systems affected?

The following version(s) are affected:

- Perforce Akana API Platform (Policy Manager console) - (Affected; specific version range not yet published in third-party reporting)

No fixed version confirmed at time of writing - consult Perforce's own advisory channel for updates

What does this mean?

Typical attack flow:

1. **Reach the Policy Manager console with a crafted request**
 - A remote, unauthenticated attacker sends a specially crafted request to the Akana Policy Manager console, exploiting a path normalization discrepancy between the authentication filter and the underlying servlet dispatcher.
2. **Bypass authentication and inject code for execution**
 - The discrepancy allows the request to bypass the authentication filter entirely and reach an endpoint that processes untrusted script code without protective measures, allowing the attacker to inject and execute arbitrary code on the server.

Attack vectors:

- A network-based, unauthenticated attack against any reachable Perforce Akana Policy Manager console.
- No user interaction or privileges are required.

Successful exploitation may allow attackers to:

- Execute arbitrary code on the server hosting the Akana Policy Manager console, without any authentication.
- Use that code execution to access, modify, or disrupt every API managed through the platform, and potentially pivot into the wider network hosting it.

Mitigation process

CERTVU recommends the following:

1. Restrict access to the Policy Manager console
 - Restrict network access to the Akana Policy Manager console to trusted administrative networks only, and ensure it is never directly reachable from the internet.
2. Monitor Perforce's advisory channel for a patch
3. Monitor for unauthorized activity on the platform
4. Apply network segmentation as defence-in-depth

Report any suspected compromised of a Perforce Akana deployment to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-85978>
2. <https://www.perforce.com/support>