

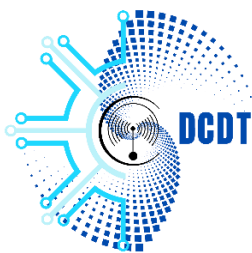
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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 291: Check Point Quantum Security Gateway VPN Certificate
Validation Flaws Leading to Unauthenticated Remote Code Execution (CVE-
2026-85102 and CVE-2026-85103).**

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 a Check Point Quantum Security Gateway, Security Management Server, or Spark Firewall with Remote Access or Site-to-Site VPN enabled. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-85102 and CVE-2026-85103 are two critical vulnerabilities in the certificate verification layer of Check Point Quantum Security Gateway, discovered during the VPN negotiation phase before authentication is finalized. Check Point is one of the world's most widely-deployed network security and firewall vendors, and Quantum Security Gateway is its flagship firewall/VPN platform used by organizations and governments globally. CVE-2026-85102 is an improper certificate trust validation flaw that may allow an unauthenticated remote attacker to execute arbitrary code on the Gateway. CVE-2026-85103 is a heap-based buffer overflow occurring during ASN.1 decoding of VPN certificates, also enabling unauthenticated remote code execution.

What are the systems affected?

The following version(s) are affected:

- Check Point Quantum Security Gateway R81.20 (Jumbo Hotfix Take 165 or below), R82 (Jumbo Hotfix Take 125 or below), and R82.10 (Jumbo Hotfix Take 43 or below) - (Affected)

R82.20 - (Not affected); R81.20/R82/R82.10 with the applicable LivePatch Take 24 or Jumbo Hotfix R82 Take 126 or later - (Not affected, patched)

What does this mean?

Typical attack flow:

1. **Reach the Gateway's VPN negotiation endpoint**
 - An unauthenticated remote attacker sends a specially crafted certificate or negotiation request to a Check Point Quantum Security Gateway's VPN service (Remote Access or Site-to-Site), before authentication is finalized.
2. **Exploit certificate validation or ASN.1 decoding flaws to execute code**
 - The crafted certificate either bypasses trust validation (CVE-2026-85102) or triggers a heap-based buffer overflow during ASN.1 decoding (CVE-2026-85103), allowing the attacker to execute arbitrary code on the Gateway itself, with no credentials or user interaction required.

Attack vectors:

- A network-based, unauthenticated attack against any Check Point Quantum Security Gateway, Security Management Server, or Spark Firewall with VPN services reachable from an untrusted network, most critically the public internet.

Successful exploitation may allow attackers to:

- Execute arbitrary code on the Check Point Gateway itself before any authentication takes place, gaining a foothold on a device that sits directly on the network perimeter.
- Use control of the Gateway to intercept, redirect, or disable VPN traffic and firewall policy, and pivot further into the internal network it is meant to protect.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch without delay

- Apply LivePatch Take 24 or Jumbo Hotfix Accumulator R82 Take 126 (as applicable to your version) per Check Point sk1000117; confirm whether your Gateway is on R82.20, which is not affected.

2. Reduce VPN exposure where patching must be delayed
3. Review VPN and gateway logs for signs of pre-authentication compromise

Report any suspected compromise of a Check Point Quantum Security Gateway, Security Management Server, or Spark Firewall to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-85102>
2. <https://www.cve.org/CVERecord?id=CVE-2026-85103>
3. <https://support.checkpoint.com/results/sk/sk1000117>