An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2609100236

# NCSC Advisory

## Critical vulnerabilites in Check Point: Quantum Security Gateway & Quantum Security Management

CVE-2026-85102, CVE-2026-85103

10th, September 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

# Description

**CVE ID:** CVE-2026-85102

**Published:** 2026-09-09

**Vendor:** Check Point

**Product:** Quantum Security Gateway

**CVSS Score[1]:** 9.8

# Products Affected

| Product | Version |
|---|---|
| Quantum Security Gateway | R81.20, R82, R82.10 |
| Quantum Security Gateway | R80, R80.10, R80.20, R80.30, R80.40, R81, R81.10 (all EoS) |
| Quantum Security Gateway | R81.10.x, R82.00.x |

# Impact

Improper certificate trust validation during VPN negotiation in Check Point Quantum Security Gateway may allow an unauthenticated remote attacker to execute arbitrary code on the Gateway.

**Common Weakness Enumeration (CWE)[2]:** CWE-295: Improper Certificate Validation.

**Known Exploited Vulnerability (KEV) catalog[3]**: No

**Used by Ransomware Operators**: N/A

# Description

[1] https://www.first.org/cvss/
[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

**CVE ID:** CVE-2026-85103

**Published:** 2026-09-09

**Vendor:** Check Point

**Product:** Quantum Security Gateway, Quantum Security Management

**CVSS Score[4]:** 9.8

# Products Affected

| Product | Version |
|---|---|
| Quantum Security Gateway, Quantum Security Management | R81.20, R82, R82.10 |
| Quantum Security Gateway, Quantum Security Management | R80, R80.10, R80.20, R80.30, R80.40, R81, R81.10 (all EoS) |
| Quantum Security Gateway, Quantum Security Management | R81.10.x, R82.00.x |

# Impact

A heap-based buffer overflow in VPN certificate ASN.1 decoding may allow an unauthenticated remote attacker to execute arbitrary code on Check Point Quantum Security Management and Quantum Security Gateway systems.

**Common Weakness Enumeration (CWE)[5]:** CWE-122: Heap-based Buffer Overflow.

**Known Exploited Vulnerability (KEV) catalog[6]**: No

**Used by Ransomware Operators**: N/A

[4] https://www.first.org/cvss/

[5] https://cwe.mitre.org

[6] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

# Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Check Point.

- https://nvd.nist.gov/vuln/detail/CVE-2026-85102
- https://www.cve.org/CVERecord?id=CVE-2026-85102
- https://support.checkpoint.com/results/sk/sk1000117
- https://nvd.nist.gov/vuln/detail/CVE-2026-85103
- https://www.cve.org/CVERecord?id=CVE-2026-85103
- https://support.checkpoint.com/results/sk/sk1000118