An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2606090209

# NCSC Advisory

## Critical Vulnerability in Checkpoint: Spark Firewalls, Quantum Security Gateway

CVE-2026-50751

**19th, June 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-2026-50751

**Published:** 2026-06-08

**Vendor:** Checkpoint

**Product:** Spark Firewalls, Quantum Security Gateway

**CVSS Score[1]:** 9.3

# Products Affected

| Product | Version |
|---|---|
| Quantum Security Gateway | R82.10 with Jumbo Hotfix Take 19 or below |
| Quantum Security Gateway | R82 with Jumbo Hotfix Take 103 or below |
| Quantum Security Gateway | R81.20 with Jumbo Hotfix Take 141 or below |
| Quantum Security Gateway | R81.10, R81, and R80.40 |
| Spark Firewalls | R80.20.X, R81.10.X, and R82.00.X |

# Impact

A logic flow weakness in Remote Access and Mobile Access certificate validation in deprecated IKEv1 key exchange allows an unauthenticated remote attacker to bypass user authentication and establish a remote access VPN connection without a valid user password.

**Common Weakness Enumeration (CWE)[2]:** CWE-287: Improper Authentication.

**Known Exploited Vulnerability (KEV) catalog[3]**: Yes

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

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

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

[3] 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 checkpoint.

- https://nvd.nist.gov/vuln/detail/CVE-2026-50751
- https://www.cve.org/CVERecord?id=CVE-2026-50751
- https://support.checkpoint.com/results/sk/sk185033
- https://blog.checkpoint.com/security/check-point-releases-important-hotfix-for-vulnerabilities-in-deprecated-ikev1-vpn-protocol/
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-50751