

Check Point VPN Products Vulnerable to Remote Code Execution via Certificate Flaw



Check Point Security Gateway and Spark Firewall products using VPN features contain a certificate validation flaw allowing unauthenticated remote attackers to execute arbitrary code.

- Vulnerability affects Check Point Security Gateway and Spark Firewall products configured with Site to Site VPN or Remote Access VPN
- Improper certificate validation allows unauthenticated remote attackers to execute arbitrary code on affected gateways
- Organizations must apply vendor mitigations immediately or discontinue product use if patches unavailable
- Internet-exposed assets require priority assessment and remediation
- CISA has issued formal guidance requiring action and forensic triage procedures

Vulnerability Overview

Check Point Security Gateway and Check Point Spark Firewall products configured with Site to Site VPN or Remote Access VPN capabilities contain an **improper certificate validation vulnerability** tracked as CVE-2026-85102. The flaw permits unauthenticated remote attackers to execute arbitrary code directly on affected gateway devices, representing a critical exposure for organizations relying on these products for secure network connectivity.

The vulnerability stems from inadequate validation of digital certificates during VPN connection establishment, allowing attackers to bypass authentication controls without requiring valid credentials or prior access to the target environment.

Regulatory and Operational Context

CISA has designated this vulnerability for mandatory remediation under its BOD 26-04 guidance on prioritizing security updates based on risk. The agency has established forensic triage requirements for affected systems and set a federal remediation deadline of 25 September 2026. Organizations are directed to apply vendor-supplied mitigations immediately or discontinue use of affected products if patches remain unavailable.

For regulated institutions in Saudi Arabia, this vulnerability presents compliance implications under frameworks requiring timely patching of critical infrastructure and secure remote access controls. The remote code execution capability and lack of authentication requirement elevate the risk profile significantly.

Immediate Response Requirements

Organizations must inventory all Check Point gateway deployments, particularly those with VPN features enabled and internet exposure. Stakeholders should evaluate each asset's exposure profile and prioritize remediation according to business criticality and attack surface. Vendor guidance must be consulted for specific mitigation steps, and forensic readiness procedures should be reviewed to ensure compliance with incident response obligations.

What to do now

1. Conduct immediate inventory of all Check Point Security Gateway and Spark Firewall deployments with VPN features enabled
2. Identify internet-facing VPN gateways and assess their exposure profile and business criticality
3. Consult Check Point vendor advisories for specific mitigation instructions and apply patches or workarounds immediately
4. If vendor mitigations are unavailable, prepare to discontinue use of affected products and implement alternative secure remote access solutions
5. Review and activate forensic triage procedures for affected systems in accordance with incident response plans

6. Document remediation actions and timelines for compliance reporting to NCA or SAMA as applicable to your sector