Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

From Zero-Day to Ransomware: Check Point VPN Bug Fuels Real-World Attacks

Date of Publication	Admiralty Code	TA Number
June 10, 2026	A1	TA2026160

Summary

First Seen: May 07, 2026
Malware: Qilin Ransomware
Affected Products: Check Point Mobile Access / SSL VPN, Check Point Remote Access VPN, Check Point Spark Firewall, Check Point Security Gateways
Impact: A critical zero-day vulnerability, tracked as CVE-2026-50751, in Check Point's Remote Access VPN and Mobile Access products has come under active exploitation, allowing attackers to bypass authentication and gain unauthorized network access without valid credentials. The flaw, rooted in the legacy IKEv1 certificate validation process, has already been used against organizations worldwide, with researchers linking at least one post-compromise intrusion to a Qilin ransomware affiliate. Check Point also disclosed a related vulnerability, CVE-2026-50752, affecting the same component, though no active exploitation has been observed. As attacks continue to rise, the campaign underscores the security risks associated with outdated VPN technologies and highlights the urgent need for organizations to apply patches and retire legacy protocols before attackers transform a simple access flaw into a full-scale network compromise.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-50751	Check Point Security Gateway Improper Authentication Vulnerability	Check Point Mobile Access / SSL VPN, Remote Access VPN, Spark Firewall	✓	✓	✓
CVE-2026-50752	Check Point Security Gateway Certificate Validation Vulnerability	Check Point Security Gateways, Spark Firewall	✗	✗	✓

Vulnerability Details

#1

Check Point has released security updates to address a critical vulnerability affecting Remote Access VPN and Mobile Access deployments that has already been exploited in zero-day attacks. Tracked as CVE-2026-50751 and classified under CWE-287 (Improper Authentication), the flaw stems from a logic error in the certificate validation process used by Check Point Remote Access VPN and Mobile Access when the legacy IKEv1 key exchange protocol is enabled. By exploiting this weakness, an unauthenticated remote attacker can bypass authentication and establish a VPN connection without valid user credentials. The issue primarily impacts environments that still allow legacy Remote Access client connections and do not enforce machine certificate authentication.

#2

The vulnerability affects products, including Check Point Mobile Access/SSL VPN, Remote Access VPN, and Spark Firewall deployments running firmware versions R80.20.X, R80.40, R81, R81.10, R81.10.X, R81.20, R82, R82.00.X, and R82.10. Check Point confirmed that CVE-2026-50751 is being actively exploited in the wild, with the earliest known attacks dating back to May 7, 2026. Exploitation activity intensified in early June and has impacted dozens of organizations worldwide. In at least one incident, post-compromise activity was linked to a Qilin ransomware affiliate. Investigators observed attackers leveraging dedicated VPS infrastructure and targeting similar VPN-related weaknesses across products from Palo Alto Networks, Fortinet, and F5.

#3

During a broader security review of the affected VPN components using Check Point's BLAST AI-powered code security platform, researchers also identified CVE-2026-50752. This vulnerability affects the same deprecated IKEv1 certificate validation mechanism and could enable a man-in-the-middle attacker to interfere with site-to-site VPN communications under specific conditions. Although the severity is rated high with a CVSS score of 7.4, Check Point has not observed any active exploitation of CVE-2026-50752. Nevertheless, the company strongly recommends applying the latest security updates to mitigate potential risks and eliminate exposure to both vulnerabilities.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-50751	Check Point Mobile Access / SSL VPN, Remote Access VPN, Spark Firewall (R80.20.X, R80.40, R81, R81.10, R81.10.X, R81.20, R82, R82.00.X, R82.10)	cpe:2.3:a:checkpoint:remote_access_vpn:*:*:*:*:*:*:*:* cpe:2.3:a:checkpoint:security_gateway:*:*:*:*:*:*:*:*	CWE-287
CVE-2026-50752	Check Point Security Gateways, Spark Firewall (R80.20.X, R80.40, R81, R81.10, R81.10.X, R81.20, R82, R82.00.X, R82.10)	cpe:2.3:a:checkpoint:security_gateway:*:*:*:*:*:*:*:*	CWE-295

Recommendations

Apply Security Hotfixes Immediately: Update all affected Check Point Security Gateways to the vendor-released hotfix without delay. This is the most direct and effective mitigation for both CVE-2026-50751 and CVE-2026-50752. Refer to Check Point SK articles sk185033 and sk185035 for exact upgrade guidance and affected configurations.

Disable Deprecated IKEv1 Key Exchange: Configure global properties for Remote Access VPN authentication to use IKEv2 only, removing support for the deprecated IKEv1 protocol. This eliminates the vulnerable code path entirely and prevents exploitation even on unpatched systems.

Remove Legacy Remote Access Client Support: Disable support for legacy Remote Access client connections and enforce Machine Certificate Authentication as mandatory for all VPN connections. This reduces the attack surface by ensuring only authorized, certificate-validated devices can establish VPN sessions.

Conduct Forensic Log Audits: Incident response teams should perform thorough forensic reviews of VPN authentication logs and gateway configurations starting from the earliest observed exploitation date of May 7, 2026. Prioritize identifying unauthorized VPN sessions, unusual connection patterns, or connections originating from VPS providers such as Kaupo Cloud HK, Shock Hosting, and Vultr Holdings.

Enable IPS and Download Latest Signatures: Activate Check Point's Intrusion Prevention System (IPS) on all affected gateways and ensure the latest signature updates are downloaded and deployed. This provides an additional layer of detection for exploitation attempts targeting CVE-2026-50751.

Upgrade End-of-Support Firmware: Organizations still running end-of-support firmware versions (R80.20.X, R80.40, R81, R81.10) should plan an accelerated migration to a currently supported release. End-of-support products receive limited security updates and represent an ongoing risk even after hotfix application.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Credential Access	T1556: Modify Authentication Process	
Command and Control	T1572: Protocol Tunneling	
	T1071: Application Layer Protocol	
Resource Development	T1583: Acquire Infrastructure	T1583.003: Virtual Private Server
	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	45[.]77[.]149[.]152, 209[.]182[.]225[.]136, 38[.]60[.]157[.]139, 162[.]33[.]177[.]101, 45[.]76[.]26[.]42, 144[.]208[.]127[.]155, 38[.]54[.]88[.]201, 38[.]54[.]107[.]167, 66[.]42[.]99[.]200, 45[.]63[.]104[.]106, 45[.]61[.]136[.]173, 146[.]71[.]81[.]184, 208[.]123[.]119[.]167, 64[.]176[.]228[.]109, 158[.]247[.]195[.]147, 144[.]208[.]127[.]134
MD5	52fda5c1b9704544f32ee98d9060e689, 51d39aa39478beeac94f2d12f682ecce
SHA256	76842bcd75b4429e2c92636274ab0395d91c441c6aea9b76fe8a051659b0c1fc

Patch Links

CVE-2026-50751:
https://support.checkpoint.com/results/sk/sk185033

CVE-2026-50752:
https://support.checkpoint.com/results/sk/sk185035

References

https://blog.checkpoint.com/security/check-point-releases-important-hotfix-for-vulnerabilities-in-deprecated-ikev1-vpn-protocol/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

June 10, 2026 • 1:00 AM

More at www.hivepro.com