Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Check Point Rushes Fixes as Two Critical Flaws Come Under Active Attack

Date of Publication	Admiralty Code	TA Number
September 23, 2026	A1	TA2026279

Summary

First Seen: July 23, 2026
Affected Products: Check Point Security Gateway, Spark Firewall (Centrally Managed), Spark Firewall (Locally Managed), Security Management Server, Multi-Domain Security Management Server, Log Server, Multi-Domain Log Server, SmartEvent
Impact: Check Point has warned of active exploitation targeting two critical vulnerabilities in its network security portfolio. CVE-2026-85102 is a pre-authentication remote code execution flaw in the Security Gateway's VPN certificate handling, where improper validation of certificate data during VPN negotiation lets an unauthenticated attacker run code on the device; it affects Security Gateway and both centrally and locally managed Spark firewalls. CVE-2026-93616 is a newly discovered zero-day in the Check Point Management web service, a pre-authentication path traversal that allows an attacker to execute a script from an arbitrary path and load an arbitrary Java class, delivering unauthenticated code execution on the server that governs firewall policy, administration, and logging. Check Point Research has confirmed real-world abuse of both: a handful of pinpointed attacks against management servers were observed as early as July 23, 2026, while broader exploitation attempts against Spark customers began on September 12, 2026, originating from anonymization infrastructure such as VPN services and proxies. No threat actor or follow-on malware has been publicly attributed. Fixes are now available for both issues, and organizations running affected versions should apply them without delay.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-93616	Check Point Multiple Products Path Traversal Vulnerability	Check Point Security Management	✓	✓	✓
CVE-2026-85102	Check Point Multiple Products Improper Certificate Validation Vulnerability	Security Gateway, Spark Firewall (Centrally Managed), Spark Firewall (Locally Managed)	✗	✓	✓

Vulnerability Details

#1

Check Point Research has confirmed active exploitation of two vulnerabilities affecting its Security Gateway and Security Management products, the more serious of which is a zero-day. CVE-2026-93616 is a pre-authentication path traversal in the Check Point Management web service. The service fails to properly constrain which files and folders a request can reach, letting an attacker break out of the intended directory and, by abusing that traversal, execute a script from an arbitrary path and load an arbitrary Java class, achieving unauthenticated code execution on the management server. Its reach extends beyond the core Security Management Server to the Multi-Domain Security Management Server, Log Server, Multi-Domain Log Server, and SmartEvent.

#2

Vulnerable versions include R82.20, R82.10 with Jumbo Hotfix Take 44 or lower, R82 with Take 126 or lower, R81.20 with Take 166 or lower, R81.10 with Take 190 or lower (end of support), and the end-of-support R80 through R81 branches. Importantly, Check Point LivePatch Take 28/29 does not remediate this issue, so administrators cannot assume a recent LivePatch leaves them protected.

#3

Check Point Research identified a handful of pinpointed attacks exploiting it as early as July 23, 2026, well before a fix was available. The advisory does not name the targeted organizations or the attackers, nor does it describe what was done after exploitation, but Check Point has published indicators of compromise and hunting guidance in support article sk1000171 so that teams can check their own systems and logs for signs of intrusion.

#4

The second flaw, CVE-2026-85102, originates in the way a Check Point gateway checks certificate data while a VPN connection is being negotiated, a weakness consistent with improper certificate validation (CWE-295). During the certificate exchange the gateway does not properly verify the certificate presented by the connecting party, so a specially crafted certificate can slip past the intended trust checks and reach code paths it should never touch. Because the flaw is exploitable before authentication, it can lead to remote code execution directly on the gateway.

#5

It affects Security Gateway and Spark firewalls, whether centrally or locally managed, across R81 and R81.10 (both end of support), R81.10.x, R81.20, R82, R82.00.x, and R82.10, and applies where Site-to-Site VPN or Remote Access VPN is in use. Check Point disclosed it and shipped fixes on September 9, 2026, with no evidence of exploitation at the time, and attempts only began on September 12, 2026, making it a rapid one-day (n-day) weaponization.

#6

The observed attempts against CVE-2026-85102 came from anonymization infrastructure such as VPN services and proxies, and used certificates whose subjects included CN=vpn,OU=users,O=global and close variants. Check Point stresses that this list is not exhaustive and that defenders should not narrow their search to only these subjects, since other certificate subjects may be in use. Fixes for both vulnerabilities are now available, and Check Point urges customers running affected versions to apply the relevant hotfixes immediately, prioritizing the actively exploited management-server zero-day CVE-2026-93616 (sk1000171) alongside the gateway fix for CVE-2026-85102 (sk1000117).

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-93616	Check Point Security Management, Multi-Domain Security Management Server, Log Server, Multi-Domain Log Server, SmartEvent (R82.20; R82.10 with Jumbo Hotfix Take 44 or lower; R82 with Take 126 or lower; R81.20 with Take 166 or lower; R81.10 with Take 190 or lower, EoS; R80, R80.10, R80.20, R80.30, R80.40, R81, all EoS)	cpe:2.3:a:checkpoint:security_management:*:*:*:*:*:*:*:*	CWE-22
CVE-2026-85102	Check Point Security Gateway, Spark Firewall Centrally Managed, Spark Firewall Locally Managed (R81, EoS; R81.10, EoS; R81.10.x; R81.20; R82; R82.00.x; R82.10)	cpe:2.3:a:checkpoint:security_gateway:*:*:*:*:*:*:*:*	CWE-295

Recommendations

Patch the Management Server Immediately: Apply the fix for CVE-2026-93616 detailed in Check Point support article sk1000171 to every affected Security Management, Multi-Domain Management, Log Server, and SmartEvent deployment. Confirm the fixed build against your exact release and Jumbo Hotfix Take, and do not rely on LivePatch Take 28/29, which does not address this flaw.

Update Affected Gateways and Spark Firewalls: Install the CVE-2026-85102 fix from support article sk1000117 on all Security Gateway and Spark firewalls, both centrally and locally managed. The fix has been available since September 9, 2026, and any device still unpatched should be treated as exposed given ongoing exploitation attempts.

Restrict Access to the Management Server: Where patching cannot happen at once, place the vulnerable management system behind a firewall and permit access only from trusted IP addresses. This can be configured through Manage & Settings, then Permissions & Administrators, then Trusted Clients in SmartConsole. Treat this strictly as a temporary measure until the fix is applied.

Apply the VPN Workaround When Patching Must Wait: For gateways that cannot yet be patched, follow Check Point's Site-to-Site VPN workaround of disabling the implied VPN rules and allowing UDP ports 500 and 4500 only from specific peer IP addresses. Note that this workaround does not apply to locally managed Spark firewalls, which must be patched.

Hunt for Signs of Compromise: Review logs for anomalous certificate-based Mobile Access logins without limiting the search to the certificate subjects listed above, and watch for suspicious logged-in users performing internal port and service scans. Use the indicators of compromise and hunting guidance in sk1000171, remembering that installing the fix does not reveal whether a server was attacked beforehand.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Links

CVE-2026-85102: https://support.checkpoint.com/results/sk/sk1000117

CVE-2026-93616: https://support.checkpoint.com/results/sk/sk1000171

References

https://blog.checkpoint.com/security/security-advisory-action-required-active-exploitation-of-cve-2026-85102-and-a-management-pre-authentication-vulnerability-cve-2026-93616/

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

September 23, 2026 • 09:00 AM

More at www.hivepro.com