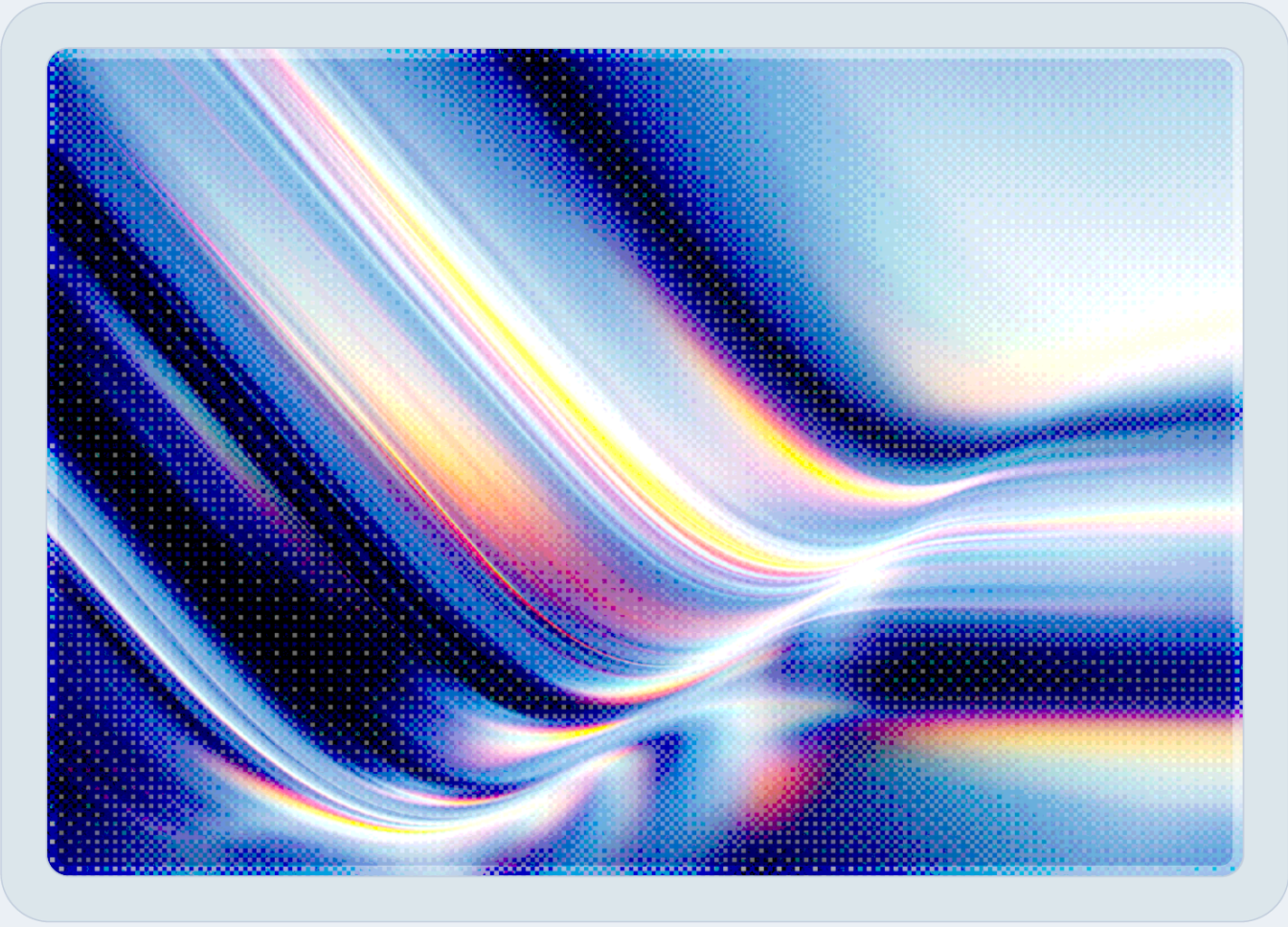
CSAI Foundation | Cloud Security Alliance

Check Point VPN Flaws: Pre-Auth RCE Risk Guidance

2026-09-15

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

Check Point disclosed two critical, unauthenticated remote code execution vulnerabilities in its VPN gateway software on September 9, 2026, both rated 9.8 on the Common Vulnerability Scoring System scale [1][2]. CVE-2026-85102 stems from improper validation of certificate trust during VPN negotiation, while CVE-2026-85103 is a heap-based buffer overflow in the ASN.1 decoder that parses VPN certificates; either flaw can let a remote attacker execute code on a Security Gateway without ever authenticating [1][3]. The Dutch National Cyber Security Centre issued an urgent public advisory on September 12, rating the likelihood and impact of exploitation as high and stating that it expects attack attempts to begin soon, even though no proof-of-concept code or in-the-wild exploitation had been confirmed at the time of writing [4][2]. Because Check Point gateways sit at the network perimeter and mediate remote access for enterprises worldwide, the exposure window between disclosure and mass patching is the period of greatest risk, and CSA assesses that organizations running affected releases should treat this as a same-day patching priority rather than a routine maintenance item.

Background

Check Point Security Gateways and Security Management Servers provide VPN termination, firewalling, and centralized policy management across many enterprise network perimeters, making them a high-value target whenever a pre-authentication flaw surfaces in their code. The current pair of vulnerabilities affects the certificate-handling logic that gateways use during VPN session negotiation, a code path that by design must be reachable by unauthenticated remote peers in order to establish encrypted tunnels [1]. That same design requirement is what makes the flaws so severe: because certificate parsing must occur before any credential exchange, a defect in that parsing logic hands an attacker a foothold before identity or access controls ever come into play.

Check Point states that it discovered both issues internally, through its own security research rather than an external report or active incident, and that it has found no indicators of compromise associated with either flaw as of publication [3]. The company published two knowledge-base advisories, sk1000117 and sk1000118, alongside patches on September 9, and it began pushing an emergency LivePatch (Take 24) to eligible gateways the same day, ahead of the jumbo hotfix releases that followed [1][4]. The Dutch NCSC's warning three days later did not report new exploitation evidence; rather, it reflected the agency's judgment that the combination of a 9.8 severity score, remote and unauthenticated

reachability, and Check Point's broad deployment across enterprise environments made rapid, opportunistic scanning and exploitation highly likely once the technical details of the patches became analyzable by attackers reverse-engineering the fix [4][2]. Vendor patch releases have, in some past cases, allowed attackers to reverse-engineer a fix and weaponize it before organizations patch. The NCSC's assessment did not cite this dynamic specifically, but rather pointed to the vulnerabilities' severity, remote and unauthenticated reachability, and Check Point's install base as the basis for its imminence rating [4][2].

The September disclosure is also not Check Point's first VPN zero-day of 2026. CVE-2026-50751, an authentication bypass affecting Remote Access VPN and Mobile Access deployments that rely on the deprecated IKEv1 key exchange protocol, was actively exploited beginning May 7, 2026, and was later linked to at least one post-compromise incident involving the Qilin ransomware operation, with a few dozen organizations targeted worldwide before Check Point issued a patch [5]. That earlier incident showed attackers moving from disclosure to real-world compromise within weeks, and it offers the closest recent precedent, in CSA's assessment, for how quickly the current pair of flaws could be weaponized once technical details circulate more widely.

Security Analysis

The two vulnerabilities are distinct in mechanism but share an attack surface: both are reachable through the VPN certificate-processing flow that a Check Point gateway executes before authenticating a remote peer. CVE-2026-85102 arises because the gateway does not properly validate certificate trust during VPN negotiation, which an attacker can exploit to have the gateway execute arbitrary code as though the certificate had been legitimately verified [1][3]. CVE-2026-85103 is a heap overflow triggered while the product decodes the ASN.1 structure of a submitted VPN certificate; a specially crafted certificate can corrupt heap memory in a way that yields remote code execution, and this flaw affects both Security Gateways and Security Management Servers rather than gateways alone [3][2]. The table below summarizes the technical distinctions relevant to triage and patch verification.

Attribute	CVE-2026-85102	CVE-2026-85103
Root cause	Improper certificate trust validation during VPN negotiation	Heap-based buffer overflow in VPN certificate ASN.1 decoder
Authentication required	None	None

Attribute	CVE-2026-85102	CVE-2026-85103
Affected components	Security Gateway	Security Gateway and Security Management Server
CVSS v3.1 score	9.8 (Critical)	9.8 (Critical)
Check Point advisory	sk1000117	sk1000118

Affected releases span the currently supported product line — R81.20, R82, R82.10, R81.10.x, and R82.00.x — as well as end-of-support versions R80 through R80.40, R81, and R81.10, which will not receive an official fix and require compensating controls or migration [1][3]. Notably, R82.20 is not affected by either flaw, which suggests the vulnerable code path was altered or removed in that later release rather than patched in place [1]. Check Point's Spark small-business firewall line is also affected, per guidance the Canadian Centre for Cyber Security amplified alongside its own advisory, underscoring that the exposure extends beyond large enterprise deployments into smaller organizations, which may have fewer dedicated security staff to track and apply vendor advisories quickly [3].

This combination — pre-authentication reachability plus a maximum CVSS score — mirrors several recent perimeter VPN and firewall vulnerabilities, in which a single memory-safety or trust-validation defect in code that must, by necessity, be exposed to the untrusted internet translated directly into full gateway compromise. The practical consequence of successful exploitation is not limited to the gateway itself. Because Check Point Security Gateways typically sit inline for all inbound remote-access traffic and often hold policy and routing authority over internal segments, an attacker who gains code execution there can pivot into internal networks, intercept or redirect VPN sessions, and disable the very security controls an organization relies on to detect follow-on activity.

Recommendations

Immediate Actions

Organizations running any affected Check Point release should apply the September 9 LivePatch (Take 24) or the corresponding jumbo hotfix — R82.10 Take 44 or later, R82 Take 126 or later, or R81.20 Take 166 or later — without waiting for a standard change-management cycle, given the NCSC's assessment that exploitation is imminent [4][1]. Spark firewall customers should confirm they are running Spark R82.00.10 Build 2325 or later, or R81.10.17 Build 4968 or later, since the small-business product line

follows a separate build-numbering scheme from the enterprise gateway [2]. Security teams should also review gateway and management server logs for anomalous VPN negotiation attempts, unexpected process crashes, or unusual certificate submissions in the days immediately following patch deployment, since post-patch reverse engineering by attackers is a common precursor to exploitation waves in comparable perimeter-device disclosures.

Short-Term Mitigations

For gateways still running end-of-support releases that will not receive a patch, the NCSC's guidance to restrict VPN access to specific, pre-approved source IP addresses rather than leaving the service open to the entire internet meaningfully reduces the population of hosts that can reach the vulnerable code path [2]. Check Point's own advisory additionally recommends disabling implied rules for VPN traffic as an interim compensating control, though several administrators have noted the guidance does not specify which configuration lines to adjust, so this step should be tested in a non-production environment before being applied broadly to avoid disrupting legitimate remote access [3]. Organizations unable to patch or restrict access immediately should consider temporarily routing remote-access traffic through a secondary, unaffected control point while remediation is completed.

Strategic Considerations

This incident is a reminder that internet-facing VPN concentrators, by the nature of the service they provide, cannot avoid exposing some pre-authentication code to the public internet, and that a single defect in that code can undermine many of the downstream access controls an organization relies on. Longer term, organizations should evaluate reducing their reliance on broadly reachable VPN gateways in favor of architectures that authenticate and authorize connections before granting any network-level reachability to internal resources. CSA's guidance on Zero Trust and Software-Defined Perimeter architectures describes exactly this shift, and it is directly applicable to the risk this incident illustrates.

CSA Resource Alignment

CSA's *An Executive View on How Zero Trust Protects Organizations by Securely Connecting Users to Resources from Anywhere* is relevant to this incident's strategic implication: it explains how Zero Trust architecture provides secure resource access while explicitly replacing traditional VPN concentrators, the same class of device whose pre-authentication attack surface is responsible for both CVE-2026-85102

and CVE-2026-85103. Organizations reassessing their remote-access architecture in light of this disclosure should treat that resource as a starting point for executive-level discussion of VPN replacement or risk reduction.

CSA's *Software-Defined Perimeter (SDP) and Zero Trust* provides technical implementation detail that complements the executive view above. SDP architectures authenticate and authorize a connection before any network-level access is granted, which eliminates the unauthenticated, pre-connection attack surface that both Check Point vulnerabilities exploit; the paper's central argument, that SDP represents the most mature implementation of Zero Trust networking, is relevant to the mitigation path for organizations seeking to reduce dependence on internet-facing VPN gateways. That shift is a multi-year architectural undertaking, however, and should be treated as a complement to immediate patching rather than a substitute for it.

Finally, the underlying issue — a critical flaw in a security product exposed to the internet, discovered and patched under time pressure — falls within the vulnerability and threat management scope of CSA's *AI Controls Matrix (AICM) v1.1*, whose Threat and Vulnerability Management domain provides control objectives for patch prioritization, exposure reduction, and compensating-control design that organizations can adapt to this incident even though the affected product itself is not an AI system.

References

[1] Bill Toulas. "Dutch NCSC: Critical Check Point VPN flaws exploitation is imminent." BleepingComputer, September 2026.

[2] Pierluigi Paganini. "Dutch NCSC Warns: Critical Check Point VPN Flaws Put Networks at Risk." Security Affairs, September 2026.

[3] The Hacker News. "Check Point Discloses Two 9.8-Rated VPN Certificate Flaws Enabling Unauthenticated RCE." The Hacker News, September 2026.

[4] Steve Zurier. "Check Point patches two critical VPN gateway bugs." SC Media, September 2026.

[5] Bill Toulas. "Check Point links VPN zero-day attacks to Qilin ransomware gang." BleepingComputer, June 2026.