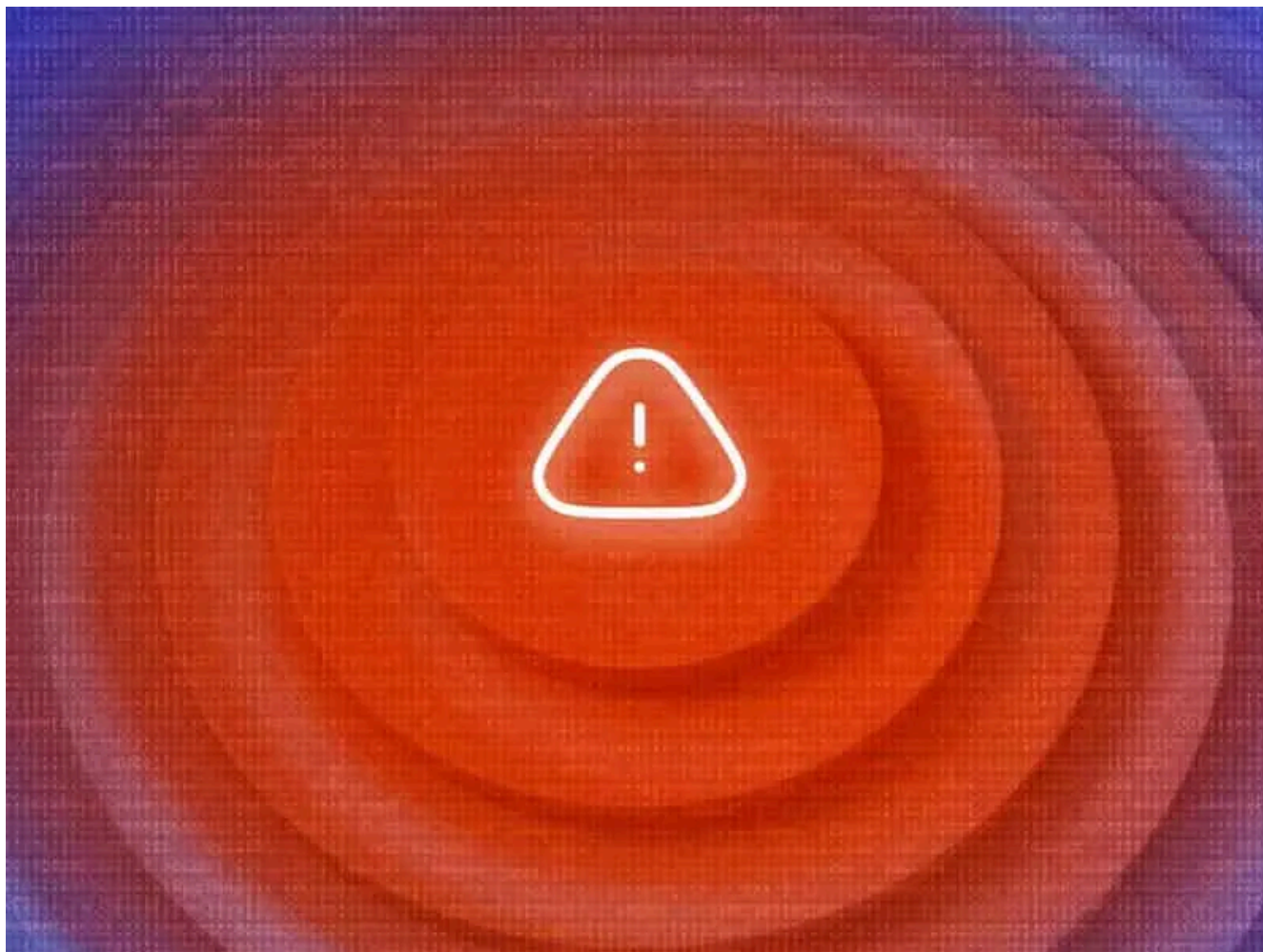


Critical Check Point VPN Zero-Day Exploited in the Wild (CVE-2026-50751)

 rapid7.com/blog/post/etr-critical-check-point-vpn-zero-day-exploited-in-the-wild-cve-2026-50751

Rapid7

June 8, 2026



Overview

On June 8, 2026, Check Point [published a security advisory](#) for [CVE-2026-50751](#), a critical authentication bypass vulnerability affecting Check Point Remote Access VPN, Mobile Access, and Spark Firewall products. The vulnerability affects deployments configured to use the deprecated IKEv1 key exchange protocol where gateways accept legacy Remote Access clients and do not require a machine certificate for connections.

CVE-2026-50751, classified as improper authentication ([CWE-287](#)), has a CVSS score of 9.3. The vulnerability stems from a logic flow weakness in how Remote Access and Mobile Access components validate certificates during IKEv1 key exchange; successful exploitation allows

an unauthenticated attacker to establish a VPN session without providing valid credentials. Per the vendor, additional post-authentication activity is required to access internal resources or escalate privileges.

Check Point has indicated that CVE-2026-50751 is being actively exploited in the wild, with observed activity dating back to May 7, 2026 and an increase in early June. The vendor characterizes the campaign as limited in scope, affecting several dozen organizations. At least one incident has been linked to a Qilin ransomware affiliate, which Check Point assesses with medium confidence. Rapid7 has observed two cases with high confidence that can be attributed to CVE-2026-50751. As of June 8, 2026, this vulnerability has been added to the CISA KEV.

Separately, during its investigation Check Point identified a related vulnerability, [CVE-2026-50752](#) (CVSS 7.4), in the same IKEv1 code path that could enable a man-in-the-middle attack against site-to-site VPN tunnels under certain configurations. No exploitation of CVE-2026-50752 has been observed.

Check Point VPN products have been targeted by zero-day vulnerabilities in the [past](#). In May 2024, [CVE-2024-24919](#), a high-severity information disclosure vulnerability in Check Point Quantum Security Gateways, was exploited in the wild and subsequently added to the CISA Known Exploited Vulnerabilities (KEV) catalog. Organizations running affected Check Point products are urged to apply the available hot fixes and follow the vendor guidance to remediate these issues.

Mitigation guidance

Check Point has released hotfixes to remediate CVE-2026-50751. Affected organizations should apply the available updates on an emergency basis, without waiting for a regular patch cycle to occur.

The following products and versions are affected (Remote Access VPN, Mobile Access / SSL VPN, Spark Firewall):

- R80.20.X (End of Support)
- R80.40 (End of Support)
- R81 (End of Support)
- R81.10 (End of Support)
- R81.10.X

- R81.20
- R82
- R82.00.X
- R82.10

Notably, four of the nine affected version branches (R80.20.X, R80.40, R81, R81.10) have reached End of Support. Organizations still running these versions should prioritize migration to a supported release.

For organizations unable to immediately apply the hotfix, Check Point has provided the following alternative mitigations:

- Remove support for the legacy remote access client
- Configure global properties for Remote Access VPN authentication to IKEv2 only
- Set machine certificate authentication as mandatory
- Enable IPS and download the latest signatures

Rapid7 strongly recommends looking for signs of compromise even after the hotfix has been applied. Per Check Point's advisory, incident response teams should prioritize forensic log audits and configuration reviews starting from May 7, 2026, the earliest known date of exploitation.

For the latest mitigation guidance, please refer to the [vendor advisory](#).

Exposure Command, InsightVM, and Nexpose

Exposure Command, InsightVM, and Nexpose customers can assess exposure to CVE-2026-50751 with a vulnerability check available in the June 9 content release.

Intelligence Hub

IntelHub customers can look into the platform to search for more details and correlate the indicators of compromise, like known malicious IPs and known post exploitation ELF payloads, with the data from their own environment.

Managed Detection Response (MDR)

The following detection rules are available for InsightIDR and Managed Detection Response (MDR) customers:

- Suspicious Network Connection - Critical Check Point VPN Zero-Day Exploited in the Wild (CVE-2026-50751)
- Suspicious Process - Critical Check Point VPN Zero-Day Exploited in the Wild (CVE-2026-50751)

Indicators of compromise

Check Point has published the following indicators associated with the CVE-2026-50751 exploitation campaign. The attacker infrastructure consists of VPS hosts from several providers (Kaupo Cloud HK, Shock Hosting, Vultr Holdings), and Check Point notes that in some cases, the VPS region matched the geography of the targeted organization.

IP addresses:

- 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

File hashes (MD5):

- 52fda5c1b9704544f32ee98d9060e689
- 51d39aa39478beeac94f2d12f682ecce

Check Point observed post-exploitation attempts to retrieve ELF payloads from attacker-controlled servers, and identified ties to the Qilin ransomware operation based on binary analysis. For the full and most current list of IOCs, please refer to the [vendor advisory](#).

Updates

- **June 8, 2026:** Initial publication.
- **June 8, 2026:** Rapid 7 observations of EITW.
- **June 9, 2026:** CVE added to CISA KEV.
- **June 10, 2026:** Updated to reflect availability of a vulnerability check and information for Intelligence Hub customers.