

Check Point VPN Authentication Bypass Under Active Exploitation

 kudelskisecurity.com/research/cve-2026-50751-check-point-vpn-authentication-bypass-under-active-exploitation

Advisory

Summary

A critical authentication bypass vulnerability (**CVE-2026-50751**) has been identified and is actively exploited in the wild against Check Point Remote Access VPN and Mobile Access deployments using the deprecated **IKEv1** key exchange protocol.

The flaw allows remote attackers to bypass user authentication by abusing a logic weakness in certificate validation, enabling VPN session establishment without valid credentials. Although additional post-authentication access is still required for deeper compromise, observed attacks have already led to targeted intrusions, including activity linked to ransomware operators.

Exploitation has been confirmed across a limited number of organizations globally, with indicators of follow-on activity associated with financially motivated threat actors.

A second vulnerability (**CVE-2026-50752**) was also identified during investigation but has not yet been observed in active exploitation.

Affected Systems and Applications

The following systems are impacted when configured with **IKEv1**:

- Check Point Remote Access VPN
- Check Point Mobile Access VPN
- Check Point Security Gateways (selected configurations)
- Check Point Spark Firewall deployments

Affected Versions

- 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

Technical Details

CVE-2026-50751 is a critical authentication bypass vulnerability with a **CVSS score of 9.3** that affects Check Point Remote Access VPN and Mobile Access components when they are configured to use the deprecated **IKEv1** key exchange protocol.

The issue originates from a logical flaw in the certificate validation process during IKEv1-based VPN authentication. Under normal circumstances, the VPN gateway is expected to strictly validate user credentials and associated certificates before establishing a secure session. However, due to this flaw, an attacker is able to manipulate the authentication flow in such a way that the validation checks can be bypassed entirely.

In practical terms, this means a remote attacker does not need to possess valid user credentials or a password to initiate and successfully establish a VPN session. By exploiting weaknesses in how certificate validation decisions are made during the IKEv1 negotiation process, the attacker can trick the system into accepting an unauthenticated connection as legitimate.

Once the VPN session is established, the attacker gains a foothold inside the internal network, effectively appearing as a valid remote user from the perspective of the VPN infrastructure.

Although the vulnerability enables authentication bypass at the VPN entry point, it does not directly grant full internal access by itself. After gaining initial VPN connectivity, the attacker still needs to perform additional post-exploitation actions to:

- Enumerate the internal environment
- Escalate privileges
- Move laterally within the network

Observations from real-world exploitation indicate that threat actors have been leveraging this initial access stage to conduct follow-on activities consistent with targeted intrusion operations, including deployment of malicious payloads and preparation for ransomware execution.

During incident analysis, Check Point Research also identified that exploitation activity has been actively occurring in the wild, with patterns suggesting a financially motivated threat

actor, including infrastructure overlaps associated with ransomware operations.

The exploitation process has been observed to rely on externally hosted virtual private server (VPS) infrastructure, which is used to initiate attacks against exposed VPN endpoints. In some cases, the geographic distribution of attacker infrastructure has been aligned with victim locations, suggesting deliberate targeting strategies.

Indicators of Compromise (IOCs)

The following indicators have been associated with observed exploitation activity targeting CVE-2026-50751 environments.

Malicious 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 Associated with Post-Exploitation Activity

52fda5c1b9704544f32ee98d9060e689
51d39aa39478beeac94f2d12f682ecce

These indicators have been linked to attacker infrastructure used in VPN exploitation attempts, including VPS-hosted systems leveraged for initial access operations and subsequent malicious activity.

Mitigation

Organizations should take immediate action to reduce exposure.

1. Apply Security Updates

Upgrade all affected Check Point Security Gateways and VPN components to the latest hotfix versions addressing:

- CVE-2026-50751
- CVE-2026-50752

2. Disable Deprecated Protocol Usage

- Disable **IKEv1** where operationally feasible.
- Migrate to **IKEv2**.

3. Review Remote Access Configuration

- Restrict VPN access policies.
- Enforce strong authentication mechanisms.
- Limit exposure of VPN gateways to trusted networks where possible.

4. Threat Hunting and Incident Response

Review VPN and authentication logs beginning **May 7, 2026** and:

- Investigate anomalous VPN session creation without corresponding valid authentication.
- Search for indicators of compromise tied to known attacker infrastructure.

5. Monitor for Compromise Indicators

- Investigate suspicious outbound connections and post-VPN login activity.
- Correlate logs with known malicious infrastructure used in attacks.

References

Official Guidance and Remediation

- <https://support.checkpoint.com/results/sk/sk185033>
- <https://support.checkpoint.com/results/sk/sk185035>

Check Point Support

<https://www.checkpoint.com/support-services/contact-support/>

Vendor Announcement

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

