



This notification is to inform you of an important security vulnerability that has been actively exploited in the wild and may affect your **Check Point VPN environment**. **Immediate action is required.**

WHAT IS THE ISSUE?

A critical security flaw (CVE-2026-50751) has been discovered in Check Point's Remote Access VPN and Mobile Access products. The vulnerability exists in an older VPN protocol called IKEv1.

An attacker can log into your VPN without needing a valid password. By exploiting a weakness in how the system checks security certificates, they can bypass authentication entirely and gain unauthorized remote access to your network.

Check Point has confirmed this is actively being exploited by attackers, including a ransomware group known as Qilin. Exploitation attempts have been observed as far back as May 7, 2026.

A second, related vulnerability (CVE-2026-50752) was also identified. This one could allow an attacker to intercept and tamper with VPN traffic between sites. It has not yet been observed in active attacks, but should still be patched.

WHAT DO YOU NEED TO DO?

1. Apply the hotfix immediately. Check Point has released security updates for all affected versions. Please update your Security Gateway as soon as possible.
2. Check your version. Affected versions include: R81.10.X, R81.20, R82, R82.00.X, R82.10, and several end-of-support versions (R80.20.X, R80.40, R81, R81.10).

Full patch guidance is available here:

<https://support.checkpoint.com/results/sk/sk185033> (CVE-2026-50751)

<https://support.checkpoint.com/results/sk/sk185035> (CVE-2026-50752)

Cloudwave SOC has already done proactive threat hunting and has not found any IoCs based on the information provided by Checkpoint.

If you have infrastructure support with Cloudwave and need assistance assessing your exposure or applying the patch, please contact us at 855-286-7787 or open a support case through our portal. You can also reach out to Check Point Support directly at:

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

This vulnerability is being actively exploited. We strongly urge you to act today.