CYBER ADVISORY

Tuesday, June 09, 2026 **CAL-CSIC-202606-A-005**

Improper Authentication Vulnerability Impacting Check Point Security Gateways and Firewalls

Unauthenticated Attacker	Logic Flow Weakness	Remote Access	Patch Available

The Cybersecurity Integration Center (CSIC) has become aware of a critical-severity authentication vulnerability impacting Check Point Security Gateways. CVE-2026-50751 carries a CVSS 3.1 score of 9.3.[1] The vulnerability stems from a logic flow weakness in certificate validation when processing connections using the deprecated IKEv1 key exchange protocol. It enables an unauthenticated attacker to exploit the logic flow weakness in the Remote Access and Mobile Access certificate validation. Successful exploitation allows an attacker to establish a remote access VPN connection without a valid user password. [2]

There have been unconfirmed reports of exploitation of CVE-2026-5075. Additionally, there has been no confirmed exploitation as a zero-day, and a Proof-of-Concept (PoC) is not publicly available. The vendor, Check Point Security, is aware of its vulnerability and has issued a patch for it, as well as guidance for mitigation if downloading and installing a patch is not immediately possible.

The Cal-CSIC recommends following Check Point Security's guidance to download and install the appropriate hot fix. If patching is not immediately possible, then please follow the guidelines for mitigation until patching can be accomplished.

For additional technical vulnerability details and Check Point Security's guidance for CVE-2026-50751, please use this link:

https://support.checkpoint.com/results/sk/sk185033

Affected Product(s) and Version(s)

Product	Version
Security Gateway	R82.10 Jumbo Hotfix Take 19 or below R82 Jumbo Hotfix Take 103 or below R81.20 Jumbo Hotfix Take 141 or below R81.10 (EOS) R81 (EOS) R80.40 (EOS)
Spark Firewalls	R80.20.X (EOS) R81.10.X R82.00.X

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: California Cybersecurity Integration Center | California Governor's Office of Emergency Services

References

[1] NVD; "CVE-2026-50751"; https://nvd.nist.gov/vuln/detail/CVE-2026-50751; accessed 08 June 2026
[2] Check Point Support Center; "CVE-2026-50751 - User Authentication bypass on VPN Remote Access and Mobile Access in deprecated IKEv1 key exchange"; https://support.checkpoint.com/results/sk/sk185033; accessed 08 June 2026