NATIONAL CSIRT-CY

User Authentication bypass on VPN Remote Access and Mobile Access in deprecated IKEv1 key exchange

Check Point

CVE-2026-50751

09 June 2026

[Cyber Threat Intelligence]

EXECUTIVE SUMMARY:

The Digital Security Authority (DSA) wants to bring to your attention high-severity authentication bypass vulnerability, **CVE-2026-50751**, has been identified in multiple versions of Check Point Remote Access VPN and Mobile Access VPN solutions and is being actively exploited in the wild.

TECHNICAL DETAILS:

A high-severity authentication bypass vulnerability, CVE-2026-50751, has been identified in multiple versions of Check Point Remote Access VPN and Mobile Access VPN solutions. The vulnerability affects deployments using the deprecated IKEv1 key exchange protocol and allows an unauthenticated attacker to establish a VPN connection without possessing a valid user password.

Check Point has confirmed that this vulnerability is being actively exploited in the wild. Successful exploitation may enable unauthorized remote access to corporate networks, potentially leading to lateral movement, data exposure, privilege escalation, and further compromise of critical systems.

Vulnerability Details

- CVE ID: CVE-2026-50751
- Severity: High
- **Vulnerability Type:** Authentication Bypass
- **Affected Components:** Check Point Remote Access VPN and Mobile Access VPN
- **Affected Platforms:** Gaia and Gaia Embedded
- **Attack Vector:** Network-based (remote exploitation)
- **Authentication Required:** No valid user password required under vulnerable configurations
- **User Interaction**: None
- **Root Cause:** Logic flow weakness in VPN certificate validation during authentication
- **Exploitation Requirements**:
    - o Remote Access VPN or Mobile Access VPN enabled
    - o IKEv1 enabled for remote access
    - o Legacy VPN clients allowed
    - o Machine certificate authentication not mandatory
- **Impact**:
    - o Bypass user authentication controls
    - o Establish unauthorized VPN connections
    - o Gain remote access to internal corporate networks
    - o Access sensitive systems and resources
    - o Facilitate lateral movement within the environment
    - o Potential data theft and further compromise
- **Exploitation Status: Actively exploited in the wild**
- **Risk Level: High, due to unauthenticated remote access and active exploitation**
- **Successful Exploitation Indicator**: Completion of a VPN Quick Mode negotiation resulting in a "Key Install" event in Check Point logs.

Vulnerable Configurations
Versions:

- 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

When (all required):

1. VPN Remote Access or Mobile Access is enabled
2. IKEv1 is enabled for remote access
3. Gateways accept legacy Remote Access clients
4. Gateways do not demand a machine certificate for connections

IOCs

Known Attacker Infrastructure: The following IP addresses have been associated with observed exploitation activity:

- 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

DETECTION GUIDANCE:

Review SmartConsole logs for:

- VPN authentication attempts from the listed IP addresses.
- IKE-related events.
- "Key Install" actions.
- Quick Mode VPN negotiations.
- Unusual remote access sessions.
- Unexpected VPN connections from unknown users or locations.

A successful exploit attempt typically results in a:

- "Key Install" event
- Successful Quick Mode negotiation

REMEDIATION:

Check Point has released hotfixes addressing CVE-2026-50751 for:

- R81.20
- R82
- R82.10
- Supported Spark Firewall releases

RECOMMENDATIONS:

The Digital Security Authority (DSA) recommends applying the mitigation or workaround provided by Check Point.

Immediate Actions:

- Search logs for IOC activity.
- Apply the latest available Jumbo Hotfix Accumulator.
- Upgrade unsupported End-of-Support versions immediately.
- Verify successful installation of vendor-provided security fixes.
- Review VPN configurations after patch deployment.
- Disable legacy client support where possible
- Rotate VPN user credentials if suspicious activity is detected.
- Review VPN access logs for anomalous sessions.
- Validate MFA deployment for remote access users.

Please ensure to distribute this information among your subsidiaries and partners and provide us with any pertinent information or findings you may have (such as Indicators of Compromise, Tactics, Techniques, and Procedures, etc.).

The Digital Security Authority (DSA) extends its appreciation for the continued collaboration.

REFERENCES:

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

DISCLAIMER:

The information presented in this report is based on available data up to the 09th of June 2026.

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.