Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0179

Kwetsbaarheden verholpen in Check Point Remote and Mobile Access VPN-producten

NCSC Security Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 16-06-2026
Revisie: 1.0.1

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Update Revisie 1

PoC code publiek beschikbaar.

Feiten

Check Point heeft kwetsbaarheden verholpen in Remote and Mobile Access VPN-producten, specifiek voor implementaties die gebruikmaken van het IKEv1 key exchange protocol.

Duiding

Er zijn twee kwetsbaarheden vastgesteld in Check Point Security Gateways en Remote Access VPN-omgevingen die gebruikmaken van het verouderde IKEv1-protocol. De kwetsbaarheden CVE-2026-50751 en CVE-2026-50752 treffen VPN-authenticatie en certificaatvalidatie. Deze kwetsbaarheden stellen aanvallers in staat om zonder geldige authenticatie toegang te verkrijgen tot VPN-omgevingen.

De kwetsbaarheid CVE-2026-50751 is als zero-day misbruikt. Volgens Check Point zou in één geval ook ransomware zijn geplaatst na dit misbruik. Het eerste gedetecteerde misbruik dateert van 7 mei. Het IKEv1-protocol is een verouderd protocol dat nog wel wordt gebruikt bij dit soort implementaties. Het NCSC-NL verwacht dat er op korte termijn grootschalig misbruik zal plaatsvinden en roept organisaties op om de advisory van Check Point op te volgen. Ook roept het NCSC-NL organisaties op om de IoC's van Check Point te controleren als binnen de organisatie betreffende producten worden gebruikt waarin IKEv1 is ingeschakeld.

UPDATE: Er is inmiddels publiek beschikbare Proof-of-Concept (PoC)-code, wat de kans op misbruik vergroot.

IOCs 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

52fda5c1b9704544f32ee98d9060e689

51d39aa39478beeac94f2d12f682ecce

Oplossingen

Check Point heeft hotfixes uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Dreigingsinformatie

IOCs 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

52fda5c1b9704544f32ee98d9060e689

51d39aa39478beeac94f2d12f682ecce

Referenties

- https://blog.checkpoint.com/security/check-point-releases-important-hotfix-for-vulnerabilities-in-deprecated-ikev1-vpn-protocol
- https://support.checkpoint.com/results/sk/sk185033
- https://support.checkpoint.com/results/sk/sk185035

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-50751	**6.9 MEDIUM**
CVE-2026-50752	**6.3 MEDIUM**

CWE's

CWE	Beschrijving
CWE-287	Improper Authentication
CWE-295	Improper Certificate Validation

Getroffen producten

checkpoint
Quantum Security Gateway
Spark Firewalls

Disclaimer