Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0365

Kwetsbaarheden verholpen in Check Point VPN-producten

NCSC Security Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 23-09-2026
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

Check Point meldt dat misbruik van de kwetsbaarheid met kenmerk CVE-2026-85102 is waargenomen. Dit is aan deze securityadvisory toegevoegd.

Feiten

Check Point heeft twee kritieke kwetsbaarheden verholpen in Quantum Security Gateway en Security Management.

Duiding

De kwetsbaarheid met kenmerk CVE-2026-85102 heeft een CVSS-score van 9,8. De kwetsbaarheid bevindt zich in het VPN-onderhandelingsproces van de Quantum Security Gateway en wordt veroorzaakt door onjuiste validatie van certificaatvertrouwen. Hierdoor kan een niet-geauthenticeerde externe aanvaller authenticatiecontroles omzeilen en willekeurige code uitvoeren op de Security Gateway. Exploitatie vindt plaats tijdens de VPN-onderhandeling, waarbij certificaatgegevens onvoldoende worden gevalideerd. De kwetsbaarheid geldt voor Security Gateway en Check Point Spark Firewall wanneer Site-to-Site VPN of Remote Access VPN wordt gebruikt.
Voor Site-to-Site VPN adviseert Check Point om implied rules for VPN uit te schakelen en VPN-toegang voor UDP/500 en UDP/4500 alleen expliciet toe te staan voor de specifieke peer-IP-adressen. Deze mitigatie is niet van toepassing op lokaal beheerde Spark Firewalls.

De kwetsbaarheid met kenmerk CVE-2026-85103 heeft een CVSS-score van 9,8. Het betreft een heap-based buffer overflow in de ASN.1-decoding van VPN-certificaten, veroorzaakt door onjuiste verwerking van ASN.1-datastructuren tijdens de certificaatverwerking. Een niet-geauthenticeerde externe aanvaller kan deze kwetsbaarheid misbruiken om willekeurige code uit te voeren op het getroffen systeem. De kwetsbaarheid bevindt zich in een component die onderdeel is van de VPN-infrastructuur en kan bij succesvolle exploitatie de vertrouwelijkheid, integriteit en beschikbaarheid van het getroffen systeem beïnvloeden.

Het NCSC verwacht dat op korte termijn pogingen tot grootschalig misbruik zullen plaatsvinden en roept organisaties op de advisory van Check Point met spoed op te volgen.

Update: Check Point meldt dat misbruik van de kwetsbaarheid met kenmerk CVE-2026-85102 is waargenomen. Het NCSC adviseert de advisory van Check Point met spoed op te volgen. Raadpleeg de blog van Check Point voor aanvullende informatie. De inschaling van deze advisory blijft ongewijzigd.

Oplossingen

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

Referenties

- https://blog.checkpoint.com/security/security-advisory-action-required-active-exploitation-of-cve-2026-85102-and-a-management-pre-authentication-vulnerability-cve-2026-93616
- https://support.checkpoint.com/results/sk/sk1000117
- https://support.checkpoint.com/results/sk/sk1000118

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-85103	9.8 CRITICAL
CVE-2026-85102	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-122	Heap-based Buffer Overflow
CWE-295	Improper Certificate Validation

Getroffen producten

checkpoint
Quantum Security Gateway
Quantum Security Management

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.