Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0238

Kwetsbaarheid verholpen in Check Point VPN producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 30-05-2024

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

Feiten

Check Point heeft een kwetsbaarheid verholpen in Quantum Gateway VPN systemen.

Check Point meldt actieve pogingen tot misbruik waar te nemen.

Duiding

Door een path-traversal-bug kan een kwaadwillende toegang krijgen tot de username- en password-gegevens van lokale accounts op het VPN-systeem. Indien deze lokale accounts, password-only zijn en geautoriseerd om een VPN-verbinding op te bouwen, kan een kwaadwillende de accounts misbruiken om door te dringen tot de interne infrastructuur. Check Point raadt af om lokale, password-only accounts te gebruiken voor VPN-autorisatie. Ook diverse best-practices adviseren om gebruikers te autoriseren via centrale authenticatie en autorisatiesystemen als AD, LDAP en RADIUS.

Bij correct, en volgens best-practices ingerichte systemen is de kans op daadwerkelijk misbruik gering.

Vanwege de media-aandacht voor deze kwetsbaarheid verwacht het NCSC wel een toename van scanverkeer en pogingen tot misbruik.

Oplossingen

Check Point heeft hotfixes uitgebracht om de kwetsbaarheid te verhelpen in de getroffen systemen.

Ook heeft Check Point uitgebreide handelingsperspectieven gepubliceerd, waarvan zij adviseert ze uit te voeren naast het inzetten van de hotfix:

- Wijzig het wachtwoord van het VPN-systeem, indien gebruik gemaakt wordt van LDAP of Active Directory.
- Blokkeer toegang van lokale accounts tot de VPN. Met name wanneer deze lokale accounts password-only zijn.

Voor meer details, zie de bijgevoegde referenties.

Referenties

› https://support.checkpoint.com/results/sk/sk182336
› https://support.checkpoint.com/results/sk/sk182337

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-24919	7.5 HIGH

CWE's

CWE	Beschrijving
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor

Getroffen producten

checkpoint
check_point_quantum_gateway_and_spark_gateway_and_cloudguard_network
cloudguard_network_security_firmware
quantum_maestro_firmware
quantum_scalable_chassis_firmware
quantum_security_gateway_firmware
quantum_spark_gateway_firmware

Disclaimer