



.....
Centre de Veille de Détection et de
Réaction aux Attaques Informatiques

BULLETIN DE SECURITE

Titre	Zero Day affectant des produits Check Point
Numéro de Référence	47663005/24
Date de Publication	30 Mai 2024
Risque	Critique
Impact	Critique

Systèmes affectés

- Quantum Maestro et Quantum Scalable Chassis versions R81.20, R81.10, R80.40, R80.30SP et R80.20SP
- Quantum Security Gateway et CloudGuard Network Security versions R81.20, R81.10, R81 et R80.40
- Quantum Spark Gateways versions R81.10.x, R80.20.x et R77.20.x

Identificateurs externes

- CVE-2024-24919

Bilan de la vulnérabilité

Un zero-day critique affectant plusieurs produits de Check Point a été corrigé. Selon Check Point, cette vulnérabilité qui affecte particulièrement l'accès VPN à ses produits vulnérables est activement exploitée et peut permettre à un attaquant d'accéder à des données confidentielles.

Solution

Veuillez se référer aux bulletins de sécurité de Check Point pour installer les mises à jour.

Risques

- Accès à des données confidentielles

Référence

Bulletins de sécurité de Check Point :

- <https://support.checkpoint.com/results/sk/sk182336>
- <https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-0353.html>
- <https://support.checkpoint.com/results/sk/sk182337>