Raport eveniment cibernetic

CVE-2024-24919

A fost identificată o vulnerabilitate în Security Gateways cu IPsec VPN, în cadrul comunității Remote Access VPN și al lamei software Mobile Access (CVE-2024-24919).

Această vulnerabilitate permite accesarea neautorizată a informațiilor sensibile stocate pe Security Gateway. În anumite scenarii, exploatarea acestei vulnerabilități poate permite unui atacator să se deplaseze lateral în rețea și să obțină privilegii de administrator de domeniu.

Recomandăm verificarea și aplicarea măsurilor de securitate adecvate pentru a preveni orice tentativă de exploatare a acestei vulnerabilități.

Informații sumare

TIP	***CVE exploatat***
Producte expuse	**Product** CloudGuard Network, Quantum Maestro, Quantum Scalable Chassis, Quantum Security Gateways, Quantum Spark Appliances **Versiune** R77.20 (EOL), R77.30 (EOL), R80.10 (EOL), R80.20 (EOL), R80.20.x, R80.20SP (EOL), R80.30 (EOL), R80.30SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x, R81.20
IOC	167[.]99.112.236 68[.]183.56.130 82[.]180.133.120
Prevenția exploatării	Pentru a asigura securitatea infrastructurii dvs., vă rugăm să efectuați următorul pas pe orice Security Gateway și Cluster care are ORICARE dintre următoarele configurații: ● Lama software IPSec VPN este activată, dar DOAR atunci când este inclusă în comunitatea Remote Access VPN. ● Lama software Mobile Access este activată. Pentru Security Gateways și membrii Cluster online, Hotfix-ul este disponibil în CPUSE. Pentru a obține Hotfix-ul, urmați pașii de mai jos: 1. Cu un browser web, conectați-vă la Gaia Portal pe Security Gateway și pe fiecare membru al Cluster-ului. 2. Instalați pachetul hotfix: Security Gateway Hotfix https://support.checkpoint.com/results/sk/sk182336

CPUSE View	Instructions
Default	a. Go to **Upgrades (CPUSE)** > **Status and Actions**. b. In the top right corner, click **Check For Updates**. c. In the **Hotfixes** section, right-click the hotfix package "**Hotfix for CVE-2024-24919**" and click **Install Update**. 
New Experience	a. Go to **Software Updates** > **Available Updates**. b. In the top right corner, click **Check for updates**. c. In the **Hotfix Updates** section, in the "**Hotfix for CVE-2024-24919**" row, click **Install**. 

	În versiunea R81.10, a fost introdusă o nouă funcționalitate pentru a îmbunătăți performanța VPN: CCCD. Această funcționalitate este dezactivată implicit și este utilizată de un număr foarte mic de Security

Pentru clienții care utilizează CCCD **(Check Point Centralized Configuration Deployment)**	Gateways la nivel global. Clienții care folosesc CCCD trebuie să dezactiveze această funcționalitate pentru ca Hotfix-ul să fie eficient. Pentru a verifica starea curentă a CCCD și pentru a o dezactiva, urmați pașii de mai jos: 1. Conectați-vă la linia de comandă (mod Expert) pe Security Gateway și pe fiecare membru al Cluster-ului. 2. Rulați comanda: **vpn cccd status** ○ Rezultatul așteptat este: **vpn: 'cccd' is disabled**. 3. Dacă rezultatul diferă, dezactivați permanent procesul CCCD rulând comanda: **vpn cccd disable** ***Notă:*** Această modificare va rămâne activă și după repornirea Security Gateway-ului.

Resurse externe

	*https://support.checkpoint.com/results/sk/sk182336*