مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Zero-Day Vulnerability- Check Point Network Security gateway products

Tracking #:432315906

Date:30-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a zero-day vulnerability in Check Point Network Security gateway products that is being actively exploited by threat actors to gain access to sensitive information on affected systems.

TECHNICAL DETAILS:

Check Point is warning a critical zero-day vulnerability (CVE-2024-24919) impacting their Network Security Gateway products.

Vulnerability Details:

- **CVE-2024-24919**
- Severity: High
- An information disclosure vulnerability exists in Check Point Security Gateways with IPSec VPN, Remote Access VPN, and the Mobile Access software blade. This vulnerability could allow an attacker to read certain information on affected devices.
- This vulnerability has been actively exploited in the wild by threat actors, primarily targeting systems with Remote Access VPN or Mobile Access enabled and configured with local accounts using password-only authentication.
- Successful exploitation of this vulnerability could allow an attacker to read sensitive information on affected Check Point security gateways.

Affected Products:

- CloudGuard Network, Quantum Maestro, Quantum Scalable Chassis, Quantum Security Gateways, Quantum Spark Appliances

Fixed Versions:

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

RECOMMENDATIONS:

- **Update Immediately:** Patch all Check Point Security Gateways with the latest available security update that addresses CVE-2024-24919.
- **Disable password-only authentication for VPN access.** Enforce multi-factor authentication (MFA) for all VPN logins.
- **Implement strong password policies.** Enforce regular password changes and minimum password complexity requirements.
- **Segment the network.** Limit access to critical systems and data.
- Monitor the network activity for suspicious behavior.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://support.checkpoint.com/results/sk/sk182336
- https://blog.checkpoint.com/security/enhance-your-vpn-security-posture