May 30, 2024

Overall Rating - High

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Check Point published a security update to address a vulnerability in the following products:

- CloudGuard Network – multiple versions
- Quantum Maestro – multiple versions
- Quantum Scalable Chassis – multiple versions
- Quantum Security Gateways – multiple versions
- Quantum Spark Appliances – multiple versions

Technical Details

Following our security update on May 27, 2024, Check Point's dedicated task force continues investigating attempts to gain unauthorized access to VPN products used by our customers. On May 28, 2024, we discovered a vulnerability in Security Gateways with IPsec VPN in Remote Access VPN community and the Mobile Access software blade (CVE-2024-24919).

These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-24919
- Check Point Security Update – sk182336
- Check Point Security