CYBER ALERT AL24-007

Summary

The Cyber Centre is aware of a critical vulnerability (CVE-2024-24919) impacting Check Point Security Gateways with IPsec VPN blade enabled and in the Remote Access VPN community or with Mobile Access blade enabled. An unauthenticated threat actor can exploit this vulnerability to access sensitive information as superuser on the device. On May 29, the Cyber Centre published AV24-305 to encourage readers to patch at their earliest opportunity.

The Cyber Centre has received reports that this vulnerability is being actively exploited.

Technical Details

The following Check Point products and versions are affected by this vulnerability:

- Products:
  - CloudGuard Network
  - Quantum Maestro
  - Quantum Scalable Chassis
  - Quantum Security Gateways
  - Quantum Spark Appliances

- Versions:
  - 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

Recommended Actions

The Cyber Centre strongly recommends that:

- Organizations using an affected device and version should ensure that the system is patched immediately [1].
- All stored credentials and certificates present on the device should be reset or revoked both on the device and the enterprise environment.

- Organizations disable unused, local VPN accounts.
- Organizations should review connection logs to identify authorized connections from unknown sources.
- Organizations should review and implement the Cyber Centre's Top 10 IT Security Actions [5] with an emphasis on the following topics:
    - Consolidating, monitoring, and defending Internet gateways.
    - Patching operating systems and applications.
    - Enforce the management of administrative privileges.
    - Segmenting and separating information.
    - Protecting information at the enterprise level.

If activity matching the content of this alert is discovered, recipients are encouraged to report via the My Cyber Portal, or email contact@cyber.gc.ca.

References

- Preventative Hotfix for CVE-2024-24919 - Quantum Gateway Information Disclosure
- Important Security Update – Stay Protected Against VPN Information Disclosure (CVE-2024-24919)
- Check Point – Wrong Check Point (CVE-2024-24919)
- N24-224 Check Point Security Advisory
- Check Point security advisory (AV24-305)
- Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089)