NCSC

National Cyber Security Centre

2405290122-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Vulnerability exists in multiple Check Point Quantum products (CVE-2024-24919)

UPDATE

Wednesday 5th June, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.*

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/.

Please treat this document in accordance with the TLP assigned.

Description

Published: 2024-05-28T19:15:00
Vendor: Check Point
Product: CloudGuard Network, Quantum Maestro, Quantum Scalable Chassis, Quantum Security Gateways, Quantum Spark Appliances
CVE ID: CVE-2024-24919
CVSS3.0 Score[1]**:** 7.5
EPSS[2]**:** 0.087230000
(For up to date EPSS score, click here: https://api.first.org/data/v1/epss?cve=CVE-2024-24919
Summary: Exploitation of this vulnerability potentially allows an attacker to read certain information on Check Point Security Gateways once connected to the internet and enabled with remote Access VPN or Mobile Access Software Blades. A Security fix that mitigates this vulnerability is available.

Products Affected

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

Versions Affected

- R80.20.x
- R80.20SP (EOL)
- R80.40 (EOL)
- R81
- R81.10
- R81.10.x
- R81.20

Impact

Exploitation of this vulnerability potentially allows an attacker to read certain information on Check Point Security Gateways once connected to the internet and enabled with remote Access VPN or Mobile Access Software Blades. The NCSC is aware that this vulnerability is currently under active exploitation.

Common Weakness Enumeration (CWE)[3]**:** CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Present in CISA Known Exploited Vulnerability(KEV)[4] **catalog:** No

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://www.first.org/epss/articles/prob_percentile_bins
[3] https://cwe.mitre.org/
[4] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from checkpoint.

For threat hunting purposes, check for the following configuration elements on Check Point systems:

- Local user accounts. Check when they were last accessed and from where.
- Disable local accounts if they are not in use.
- Local accounts should have multiple layers of security such as such as certificates and not just password-only options.

Check Point has released a script to check Security Gateways for CVE-2024-24919. Users can download the script if they have a Check Point login from the following: https://support.checkpoint.com/results/download/133115

Additional recommendations and mitigation's for CVE-2024-24919 can be found in the respective link(s) below: https://support.checkpoint.com/results/sk/sk182336

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie