Security Advisory 2024-053

Zero-day Vulnerability in Check Point Security Gateways

May 30, 2024 — v1.0

TLP:CLEAR

History:

- *30/05/2024 — v1.0 – Initial publication*

Summary

On May 28, 2024, Check Point issued an advisory about a zero-day vulnerability, **CVE-2024-24919**, affecting Check Point Security Gateways. This high-severity information disclosure vulnerability can be exploited to gain unauthorised access to sensitive information on systems with remote Access VPN or Mobile Access Software Blades enabled [1].

It is recommended applying the hotfix and the extra protection measures provided by the vendor on affected devices.

Technical Details

Tracked as **CVE-2024-24919**, the high-severity information disclosure vulnerability enables attackers to read certain information on internet-exposed Check Point Security Gateways with remote Access VPN or Mobile Access Software Blades enabled [1].

Affected Products

Check Point has released the following security updates to address the flaw [1]:

- Quantum Security Gateway and CloudGuard Network Security: 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: R81.10.x, R80.20.x, R77.20.x

Recommendations

CERT-EU recommends applying the hotfix and the extra protection measures on affected devices as soon as possible [2].

Extra Protection Measures

As described in Check Point's advisory, it is strongly recommended [2]:

- changing the password of the Security Gateway's account in Active Directory;
- preventing local accounts from connecting to VPN with password authentication.

Upon taking these actions, it is also recommended reviewing the authentication logs for those local accounts to identify any suspicious connection.

References

[1] https://www.bleepingcomputer.com/news/security/check-point-releases-emergency-fix-for-vpn-zero-day-exploited-in-attacks/

[2] https://support.checkpoint.com/results/sk/sk182336