CYBER ADVISORY

TLP:CLEAR
29 May 2024

Check Point Network Security Zero-Day

CVE-2024-24919 | Check Point | Zero-Day | Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability under active exploitation known as CVE-2024-24919.[1] The vulnerability affects Check Point's CloudGuard Network, Quantum Maestro, Quantum Scalable Chassis, Quantum Security Gateways and Quantum Spark Appliances.[2] Exploitation of the information disclosure vulnerability may allow an attacker to access certain information on internet-connected Gateways which have been configured with IPSec VPN, remote access VPN or mobile access software blade.[3]

The Cal-CSIC recommends to immediately apply the appropriate hotfix for the affected Check Point product.

For further information on applying hotfixes, please refer to Check Point Support Center.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.

Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] The Hacker News; "Check Point Warns of Zero-Day Attacks on its VPN Gateway Products;" https://thehackernews.com/2024/05/check-point-warns-of-zero-day-attacks.html; accessed 29 May 2024

[2] National Vulnerability Database; "CVE-2024-24919 Detail;" https://nvd.nist.gov/vuln/detail/CVE-2024-24919; accessed 29 May 2024

[3] Tenable; "CVE-2024-24919: Check Point Security Gateway Information Disclosure Zero-Day Exploited in the Wild;" https://www.tenable.com/blog/cve-2024-24919-check-point-security-gateway-information-disclosure-zero-day-exploited-in-the; accessed 29 May 2024