

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Check Point Fixes Zero-Day CVE-2024-24919 Exploited in the Wild

Date of Publication

May 30, 2024

Admiralty Code

A1

TA Number

TA2024212




Summary

First Seen: April 30, 2024

Affected Product: Check Point Security Gateway

Impact: CVE-2024-24919 is a zero-day vulnerability in Check Point Security Gateways that allows attackers to read sensitive information when remote Access VPN or Mobile Access Software Blades are enabled. This vulnerability has been exploited in the wild since April 30, 2024, to steal Active Directory data. Check Point has released hotfixes for affected versions, and users are advised to update their AD passwords if they cannot apply the patches immediately

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-24919	Check Point Security Gateway Information Disclosure Vulnerability	Check Point Security Gateway			

Vulnerability Details

#1

CVE-2024-24919 is a zero-day vulnerability identified in Check Point Security Gateways that could allow an attacker to read certain information when the gateway is connected to the internet and has remote Access VPN or Mobile Access Software Blades enabled. This vulnerability can potentially be exploited by malicious users to gain access to sensitive information.

#2

Check Point has released hotfixes to address this issue across various versions of their software, including R81.20, R81.10, and R81. The vulnerability was particularly concerning because it has been actively exploited in the wild since at least April 30, 2024, with attackers using it to extract password hashes of local accounts, including Active Directory service account, and further stealing Active Directory data and move laterally within networks.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-24919	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	cpe:2.3:a:checkpoint:quantum_gateway:*:*:*:*:*	CWE-200

Recommendations



Apply Hotfixes: Administrators need to apply hotfixes by ensuring all Security Gateways with IPsec VPN, Remote Access VPN, or Mobile Access software blades enabled are updated with the latest hotfixes. This can be done through the Gaia Portal under Software Updates > Available Updates > Hotfix Updates. After selecting and installing the appropriate hotfix for their version, they should reboot the Security Gateway.



Manual Hotfix Installation: For end-of-life (EOL) versions, administrators must download the hotfix manually from Check Point's support page and follow the manual installation instructions provided in Check Point's security bulletin.



Security Enhancement: Renew the Security Gateway's outbound SSL inspection CA certificate and inbound SSL inspection server certificates, and reset all Gaia OS admin, local users, and Expert mode passwords to enhance overall security and prevent exploitation of the CVE-2024-24919 vulnerability.



Enhance Authentication Security: Administrators should update the Active Directory password used by the Security Gateway's account if it is configured to use LDAP Account Unit, following the instructions in the Check Point security bulletin. Additionally, they should prevent weak authentication by avoiding the use of local accounts with password-only authentication for VPN access, opting for strong, multi-factor authentication methods whenever possible.



Vulnerability Scanning: Conduct regular vulnerability scans on your network to identify any potential weaknesses or unpatched software. This proactive approach allows you to address security issues promptly before they can be exploited by attackers.

Potential MITRE ATT&CK TTPs

<u>TA0006</u> Credential Access	<u>TA0001</u> Initial Access	<u>TA0042</u> Resource Development	<u>TA0010</u> Exfiltration
<u>TA0009</u> Collection	<u>T1588.006</u> Vulnerabilities	<u>T1588.005</u> Exploits	<u>T1133</u> External Remote Services
<u>T1005</u> Data from Local System	<u>T1110.002</u> Password Cracking	<u>T1212</u> Exploitation for Credential Access	<u>T1110</u> Brute Force
<u>T1190</u> Exploit Public-Facing Application	<u>T1588</u> Obtain Capabilities		

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	23[.]227[.]196[.]88, 23[.]227[.]203[.]36, 37[.]19[.]205[.]180, 38[.]180[.]54[.]104, 38[.]180[.]54[.]168, 46[.]59[.]10[.]72, 46[.]183[.]221[.]194,

TYPE	VALUE
IPv4	46[.]183[.]221[.]197, 64[.]176[.]196[.]84, 87[.]206[.]110[.]89, 104[.]207[.]149[.]95, 109[.]134[.]69[.]241, 146[.]70[.]205[.]62, 146[.]70[.]205[.]188, 149[.]88[.]22[.]67, 154[.]47[.]23[.]111, 156[.]146[.]56[.]136, 158[.]62[.]16[.]45, 167[.]61[.]244[.]201, 178[.]236[.]234[.]123, 185[.]213[.]20[.]20, 185[.]217[.]0[.]242, 192[.]71[.]26[.]106, 195[.]14[.]123[.]132, 203[.]160[.]68[.]12, 68[.]183[.]56[.]130, 167[.]99[.]112[.]236, 132[.]147[.]86[.]201, 162[.]158[.]162[.]254, 61[.]92[.]2[.]219, 183[.]96[.]10[.]14, 198[.]44[.]211[.]76, 221[.]154[.]174[.]74, 112[.]163[.]100[.]151, 103[.]61[.]139[.]226, 82[.]180[.]133[.]120, 146[.]185[.]207[.]0/24, 193[.]233[.]128[.]0/22, 193[.]233[.]216[.]0/21, 217[.]145[.]225[.]0/24, 31[.]134[.]0[.]0/20, 37[.]9[.]40[.]0/21, 45[.]135[.]1[.]0/24, 45[.]135[.]2[.]0/23, 45[.]155[.]166[.]0/23, 5[.]188[.]218[.]0/23, 85[.]239[.]42[.]0/23, 88[.]218[.]44[.]0/24, 91[.]132[.]198[.]0/24, 91[.]218[.]122[.]0/23, 91[.]245[.]236[.]0/24, 87[.]120[.]8[.]173

Patch Details

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

Link:

<https://support.checkpoint.com/results/sk/sk182336>

References

<https://blog.checkpoint.com/security/enhance-your-vpn-security-posture>

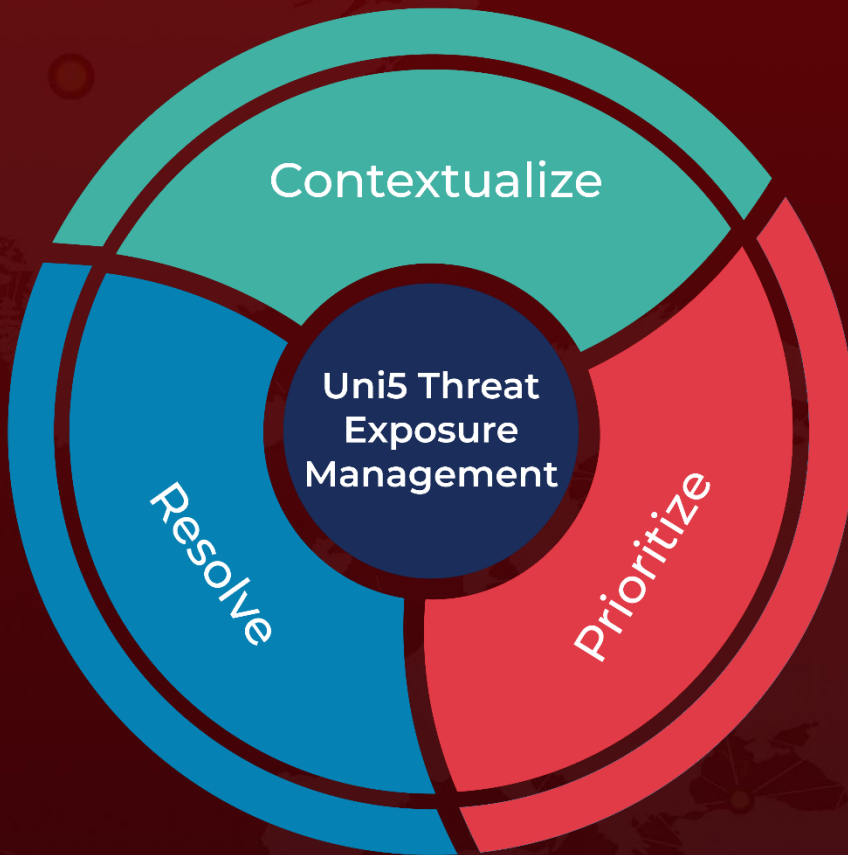
<https://support.checkpoint.com/results/sk/sk182337>

<https://www.mnemonic.io/resources/blog/advisory-check-point-remote-access-vpn-vulnerability-cve-2024-24919/>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

May 30, 2024 • 5:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com