Author: Jack Fitzgerald

Official Incident Report

Date: Jun, 06, 2024, 03:12 PM

Event ID: 263

Rule Name: SOC287 - Arbitrary File Read on Checkpoint Security Gateway [CVE-2024-24919]

Table of Contents

Alert Details

Severity: High

Type: Web Attack

Hostname: CP-Spark-Gateway-01

Destination IP Address: 172.16.20.146

Source IP Address: 203.160.68.12

HTTP Request Method: POST

Requested URL: 172.16.20.146/clients/MyCRL

Request: aCSHELL/../../../../../../../../../../etc/passwd

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:126.0) Gecko/20100101 Firefox/126.0

Alert Trigger Reason: Characteristics exploit pattern Detected on Request, indicative exploitation of the CVE-2024-24919.

Device Action: Allowed

Based on the information provided in the alert, it appears that an attacker has performed an **arbitrary file read** on **checkpoint security gateway** host **172.16.20.146**. The alert is triggered by rule SOC287 - Arbitrary File Read on Checkpoint Security Gateway [CVE-2024-24919].

CVE-2024-24919 is a **zero-day arbitrary file read** in **Check Point Security Gateways**.

The device action is marked **allowed**, indicating that the arbitrary file read was performed on the host machine.

Overall, it appears that the **alert** may be suspicious, and further investigation is needed to identify the extent of the alert and determine if any necessary actions are required to remediate the situation.

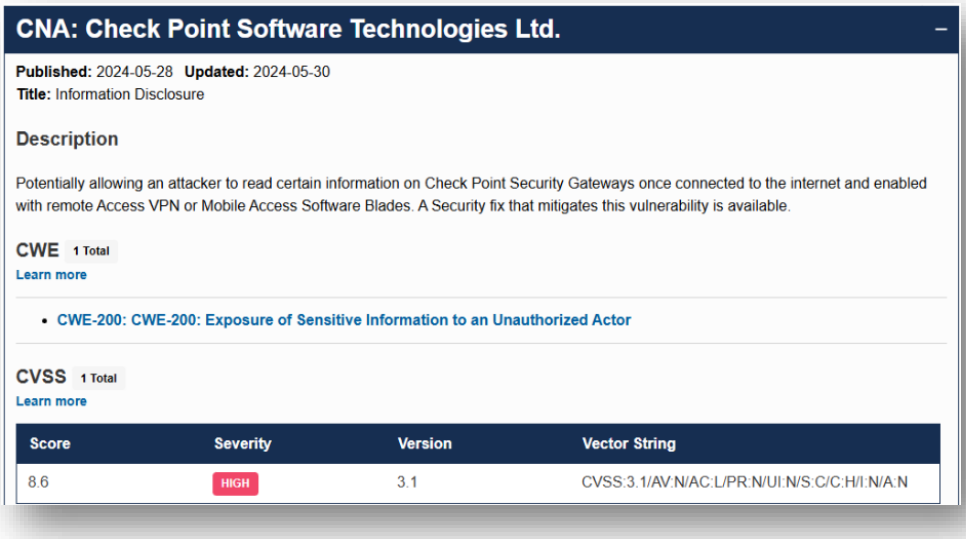
Detection

Verify

As a security analyst, one of the first steps we take to verify the alert and determine whether it is a **false positive** or a **true positive** incident is to analyse the logs collected from the host by our security products.

First, we need to understand what **CVE-2024-24919** represents.

https://www.cve.org/CVERecord?id=CVE-2024-24919



CNA: Check Point Software Technologies Ltd.

Published: 2024-05-28 **Updated:** 2024-05-30
Title: Information Disclosure

Description

Potentially allowing 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.

CWE 1 Total
Learn more

- CWE-200: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

CVSS 1 Total
Learn more

Score	Severity	Version	Vector String
8.6	HIGH	3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

Next, we need to understand why the alert was triggered.

Rule Name: **Arbitrary File Read** on Checkpoint Security Gateway

CVE: CVE-2024-24919 – **Information Disclosure**

Alert Trigger Reason: Characteristics exploit pattern Detected on Request, **indicative exploitation of the CVE-2024-24919**

Next, we need to collect some relevant data about the attack.

Destination IP Address: **172.16.20.146**

- Hostname: **CP-Spark-Gateway-01**
- User-Agent: Mozilla/5.0 (Macintosh; Intel **Mac OS X** 10.15; rv:126.0) Gecko/20100101 **Firefox**/126.0
- Domain: **LetsDefend**
- Primary User: **admin**
- Last Login: **Jun, 05, 2024, 09:05 AM**

Next, we should examine the HTTP traffic to understand what sort of web attack is occurring.

RFI/LFI attack via **Path Traversal** resulting in **Arbitrary File Read**:

- HTTP Request Method: **POST**
- Requested URL: **172.16.20.146/clients/MyCRL**
- Request: **aCSHELL/../../../../../../../../../../etc/passwd**

Our final step of the detection phase is to check whether the attack was successful.

Investigating Log Analysis for **203.160.68.12**:

- [06/Jun/2024:15:12:45 +0000] "POST /clients/MyCRL HTTP/1.1" 200 1256 "aCSHELL/../../../../../../../../../../etc/passwd" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:126.0) Gecko/20100101 Firefox/126.0"

The HTTP status 200 and response size indicate the attack was **successful**.

Analysis

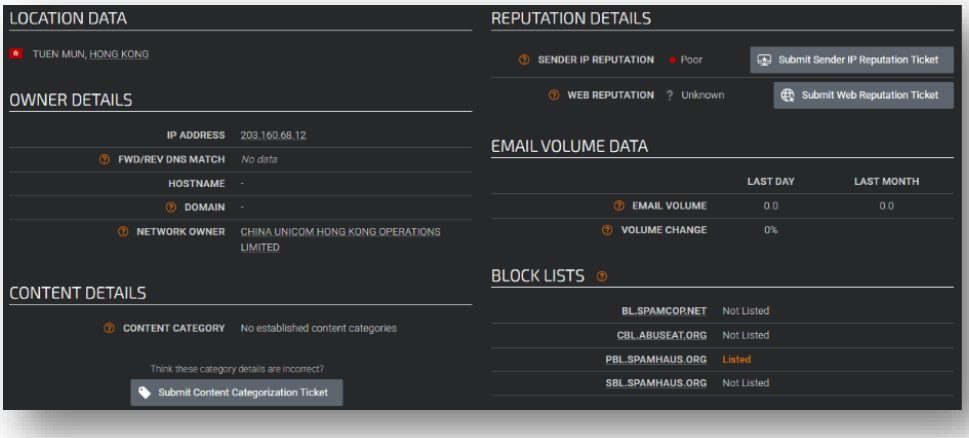
The next step of our investigation into this Path Traversal web attack is to analyse the IP address of the attacker using **VirusTotal**, **AbuseIPDB**, and **Talos Intelligence**.

https://www.virustotal.com/gui/ip-address/203.160.68.12

1/95 security vendor flagged this IP address as malicious

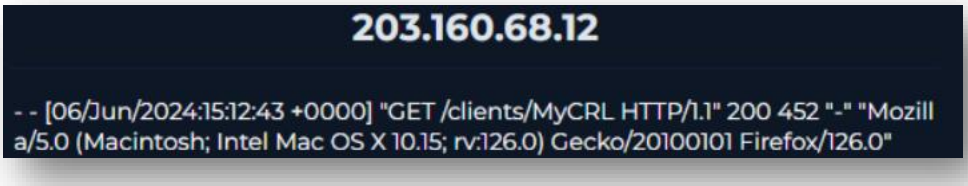
https://www.abuseipdb.com/check/203.160.68.12

https://talosintelligence.com/reputation_center/lookup?search=203.160.68.12



Next, we can investigate the logs of the incident. We found that 1 event (before Jun, 06, 2024, 03:30 PM UTC) originating from this alert, being accessed from a LOGFILE.

The first log we find seems to be a successful GET Request from **203.160.68.12** from a Firefox 126 browser on macOS to **/clients/MyCRL**.



The second log we find seems to be a direct exploitation attempt, payload indicates **Path Traversal/LFI** attack on **/etc/passwd** from the **same address**, correlated with the

previous GET Request log, a **CSHELL** keyword is a **known exploit pattern** used to test for **shell injection vulnerabilities**, attempting to **access a shell handler**.

The third log we find seems to be an **unsuccessful** attempt to perform **Path Traversal** to access **/etc/shadow**, given POST Response 403 Forbidden.

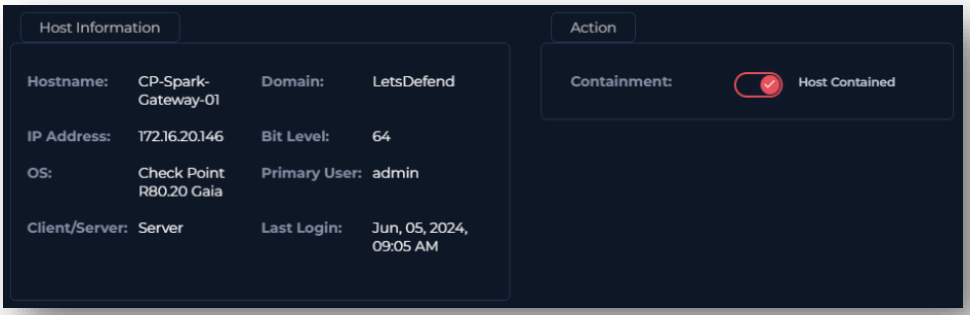
The fourth log we find seems to be the **same address**, trying a **pivot-to-root** attack behavior with **no payload** to see what the server returns.

From these analyses, we can conclude that the attacker's **Path Traversal** attack was **unsuccessful**, due to HTTP Response Status: 403 (access not granted).

However, the **pivot-to-root** attack may have been **successful**.

Containment

Based on the information gathered during the investigation, it is highly likely that the system has been compromised. Immediate isolation of the system from the network is required, and the matter is to be escalated to Tier 2.



Summary

The incident involves a compromised system named **CP-Spark-Gateway-01** with an IP address of **172.16.20.146**. The alert was triggered by the detection of an **arbitrary file read** with behaviour linked to **CVE-2024-24919**, based on the rule SOC287 - Arbitrary File Read on Checkpoint Security Gateway [CVE-2024-24919].

Upon further analysis, it was discovered that **CVE-2024-24919** is a zero-day arbitrary file read in Check Point Security Gateways.

The attacker **203.160.68.12** Requested URL **172.16.20.146/clients/MyCRL** with a Path Traversal/LFI attack to request **aCSHELL/../../../../../../../../../../etc/passwd**.

203.160.68.12 was successful in performing Path Traversal/LFI attack on **172.16.20.146** to preform an **arbitrary file read** on **/etc/passwd**.

However, **203.160.68.12** was **unsuccessful** in performing **Path Traversal/LFI** attack to perform an arbitrary file read on **/etc/shadow**. Tier 2 Escalation Required - Endpoint Contained.

Immediate action needs to be taken to isolate the compromised system; Tier 2 escalation is required, and the event was identified as a **True Positive**.

Lessons Learned

- The attacks primarily succeeded by leveraging local user accounts configured with weak, password-only authentication, a practice not recommended by the vendor

- The presence of MFA significantly mitigates the impact of compromised credentials, as stolen password hashes alone would be insufficient for an attacker to gain access

- The initial vendor advisory described the flaw vaguely as an information disclosure vulnerability, but security researchers quickly determined it was a more severe arbitrary file read that could lead to unauthenticated remote code execution in certain scenarios

Remediation Actions

- Install the specific security updates

- Check logs for POST requests to /clients/MyCRL with directory traversal attempts (../) or suspicious Linux paths

- Look for authorized connections from unknown sources or activity from known malicious IPs

Appendix

MITRE ATT&CK

MITRE Tactics	MITRE Techniques
Initial Access	T1190 - Exploit Public-Facing Application
Discovery	T1083 - File and Directory Discovery

Artifacts

Value	Comment	Type
172.16.20.146/clients/MyCRL	Targeted URL	URL Address
203.160.68.12	Attacker source address	IP Address

LetsDefend Playbook

LetsDefend Event ID: 263