EventID@263 - SOC287 - Arbitrary File Read on Checkpoint Security Gateway - CVE-2024-24919

Executive Summary

This alert was triggered for **CVE-2024-24919**, a **high-severityzero-dayvulnerability** impacting **CheckPointSecurityGateways** that have **RemoteAccessVPN** or **MobileAccessSoftware Blades** enabled.
It allows **unauthenticatedremoteattackers** to perform **arbitraryfilereads** via a **pathtraversalflaw**, potentially exposing sensitive files and credentials.

Analysis of the event logs shows an external attacker (IP: **203.160.68.12**, located in **Hong Kong**) attempting to exploit this vulnerability to read /etc/passwd and /etc/shadow on the internal host `CP-Spark-Gateway-01`.
The attack successfully retrieved /etc/passwd but failed when attempting /etc/shadow.

---

1. Event Information

Field	Details
Event ID	263 SOC287 — Arbitrary File Read on Check Point Security Gateway [CVE-2024-24919]
Rule Name	
Event Time	June 06 2024 03:12 PM
Severity	High
Hostname	CP-Spark-Gateway-01
Destination IP	172.16.20.146
Source IP	203.160.68.12
HTTP Method	POST
Requested URL	`/clients/MyCRL`
Request Body	`aCSHELL/../../../../../../../../../../etc/passwd`
User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:126.0) Gecko/20100101 Firefox/126.0
Action Taken	Allowed

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

EventID :	263
Event Time :	Jun, 06, 2024, 03:12 PM
Rule :	SOC287 - Arbitrary File Read on Checkpoint Security Gateway [CVE-2024-24919]
Level :	Security Analyst
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

Show Hint

---

2. Vulnerability Background

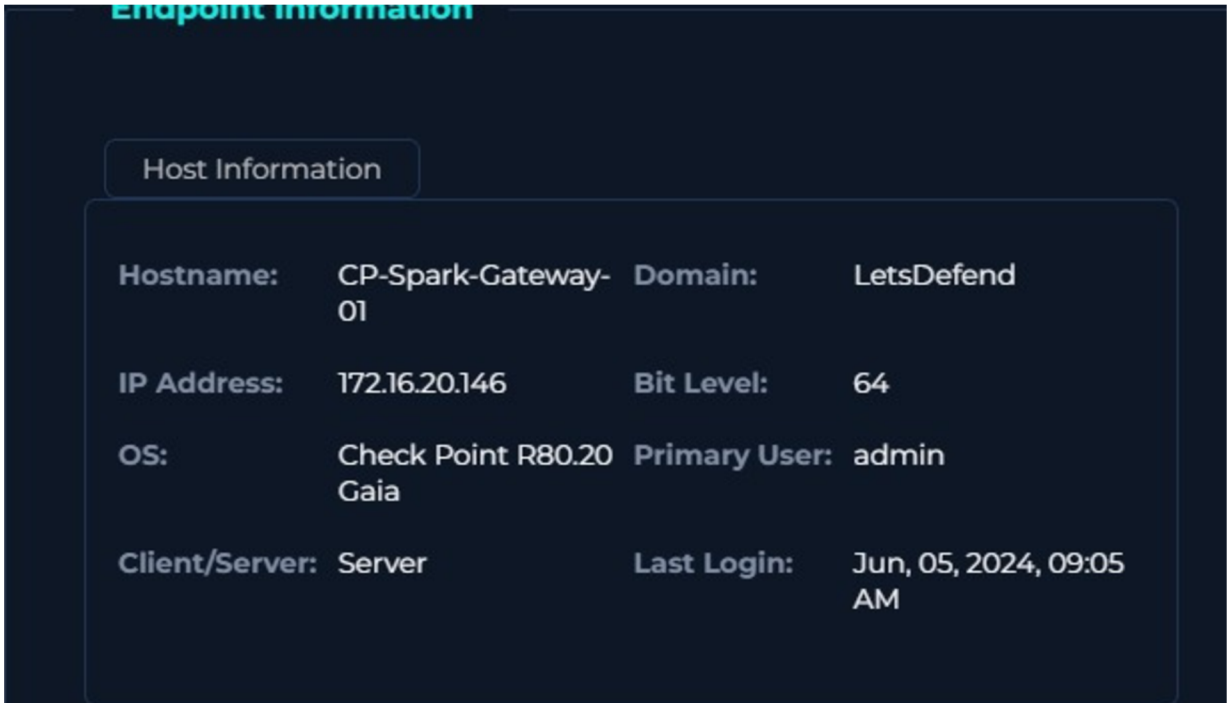
- **CVE ID:**CVE-2024-24919
- **CVSS Score:** 8.0 (High)
- **Type:** Arbitrary File Read / Path Traversal
- **Affected Products:** Check Point Security Gateway with Remote Access VPN or Mobile Access Software Blades
- **Impact:** Exposure of sensitive system files, credentials, potential RCE
- **Remediation:** Upgrade to fixed firmware / apply Check Point hotfix

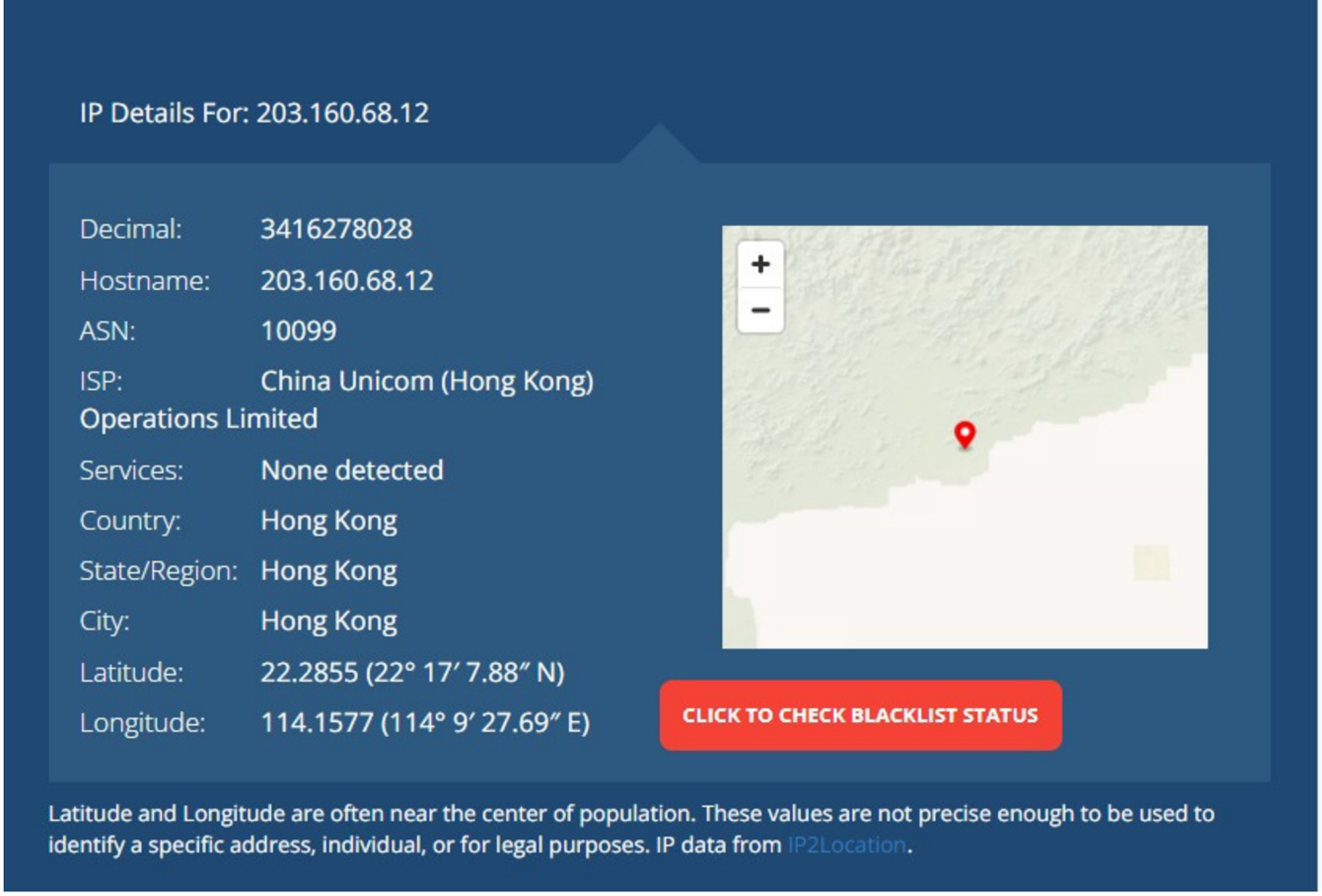
---

3. Network Entities

Role	IP Address	Host / Details
Source (Attacker)	203.160.68.12	China Unicom (Hong Kong) Operations Ltd • ASN AS10099 • Hosting Provider
Destination (Target)	172.16.20.146	CP-Spark-Gateway-01 (R80.20 Gaia) • Primary user: admin

> Traffic direction: **External** → **Internal** (Internet → Corporate Network)





---

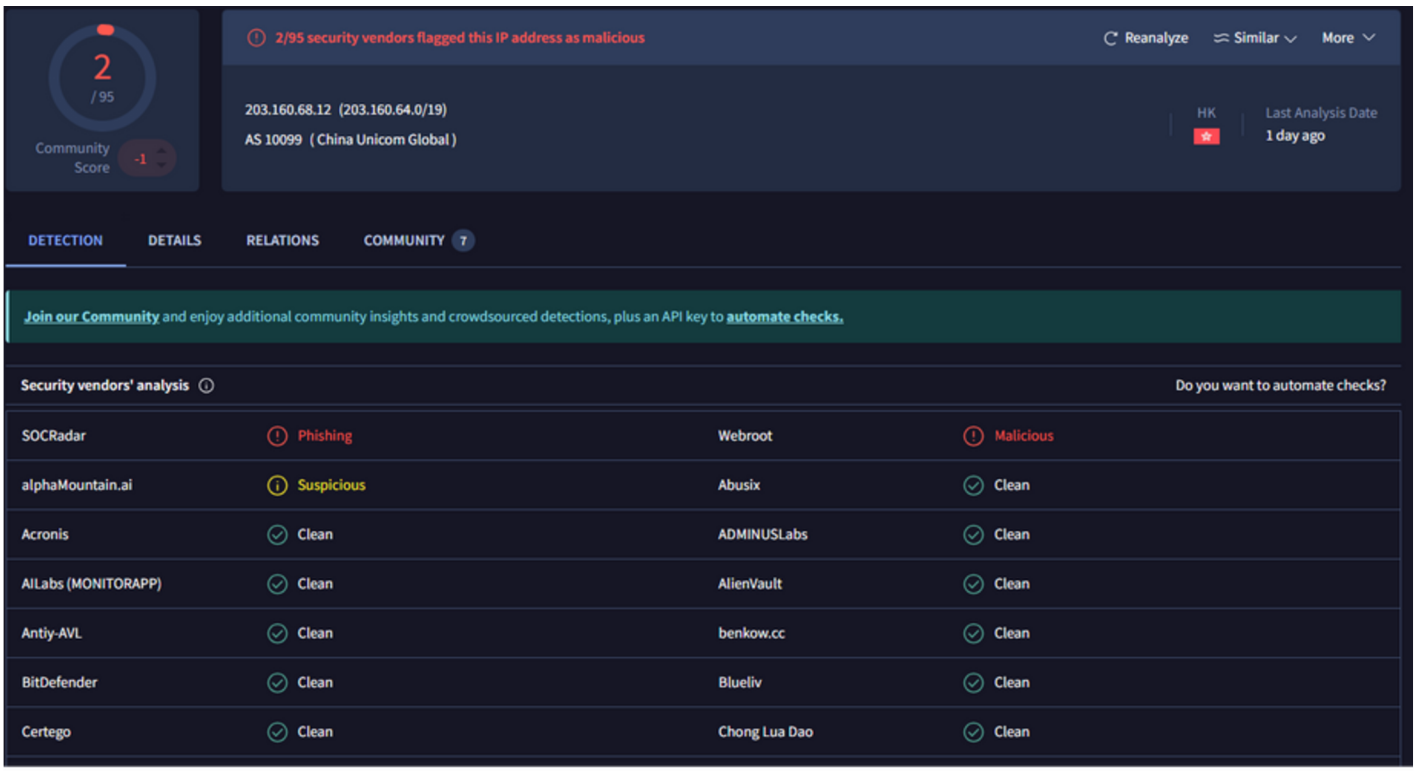
4. Investigation Steps

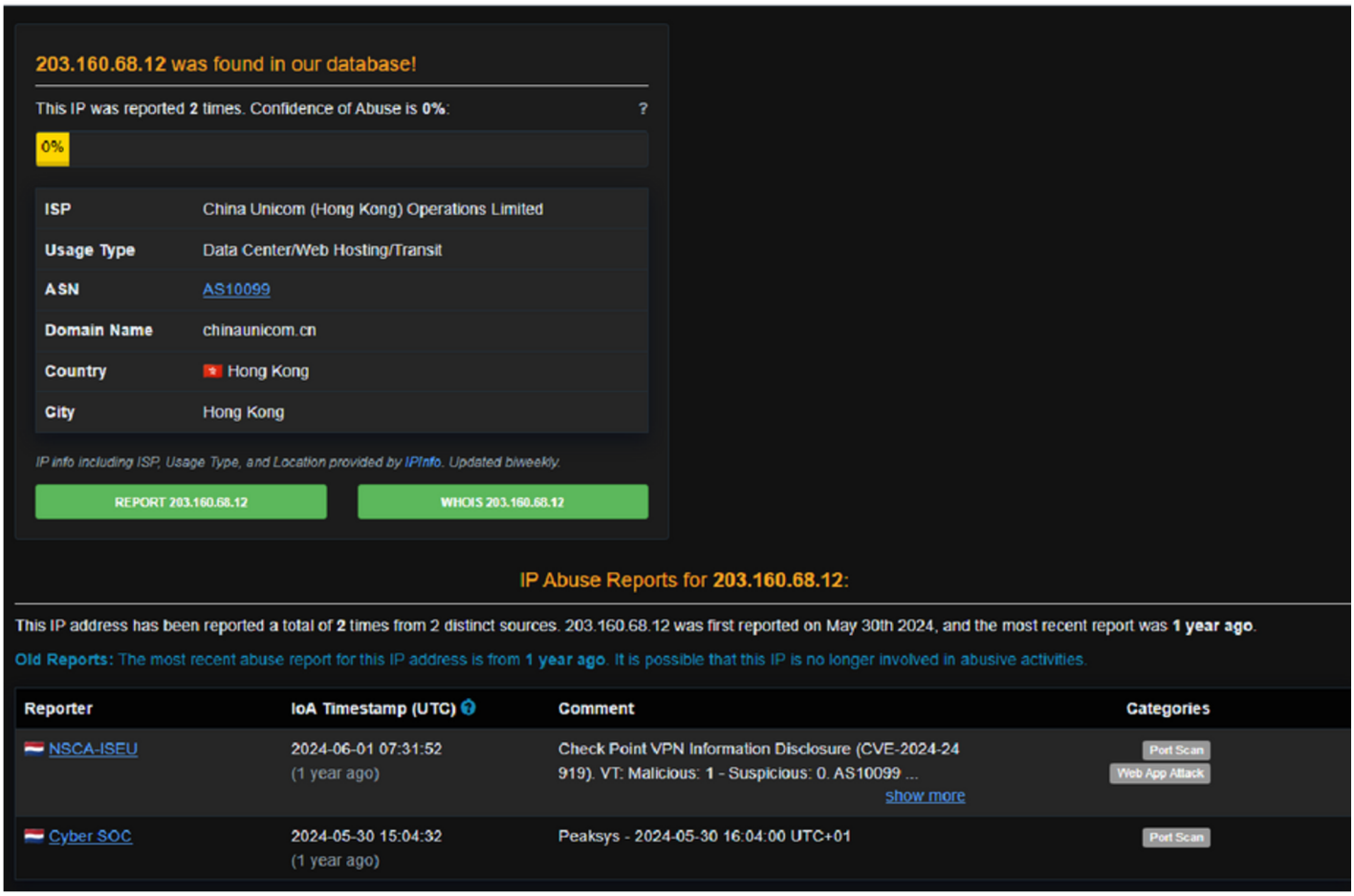
Step 1 — Initial Alert Review

- The alert **SOC287** flagged an **arbitrary file read attempt** via an HTTP POST request to `/clients/MyCRL`.
- The payload contained **directory traversal sequences (`../../../../`)**, characteristic of **Local File Inclusion (LFI)** and **path traversal** exploits.

Step 2 — Source IP Reputation Check

- **AbuseIPDB:** Two historical abuse reports (port scan, web app attack linked to CVE-2024-24919).
- **VirusTotal:** 2 vendors flagged the IP as *suspicious/phishing*.
- **Conclusion:** The IP has a low confidence of abuse but is associated with previous malicious activity against VPN gateways.





IP Abuse Reports for 203.160.68.12:

This IP address has been reported a total of **2** times from 2 distinct sources. 203.160.68.12 was first reported on May 30th 2024, and the most recent report was **1 year ago**.

Old Reports: The most recent abuse report for this IP address is from **1 year ago**. It is possible that this IP is no longer involved in abusive activities.

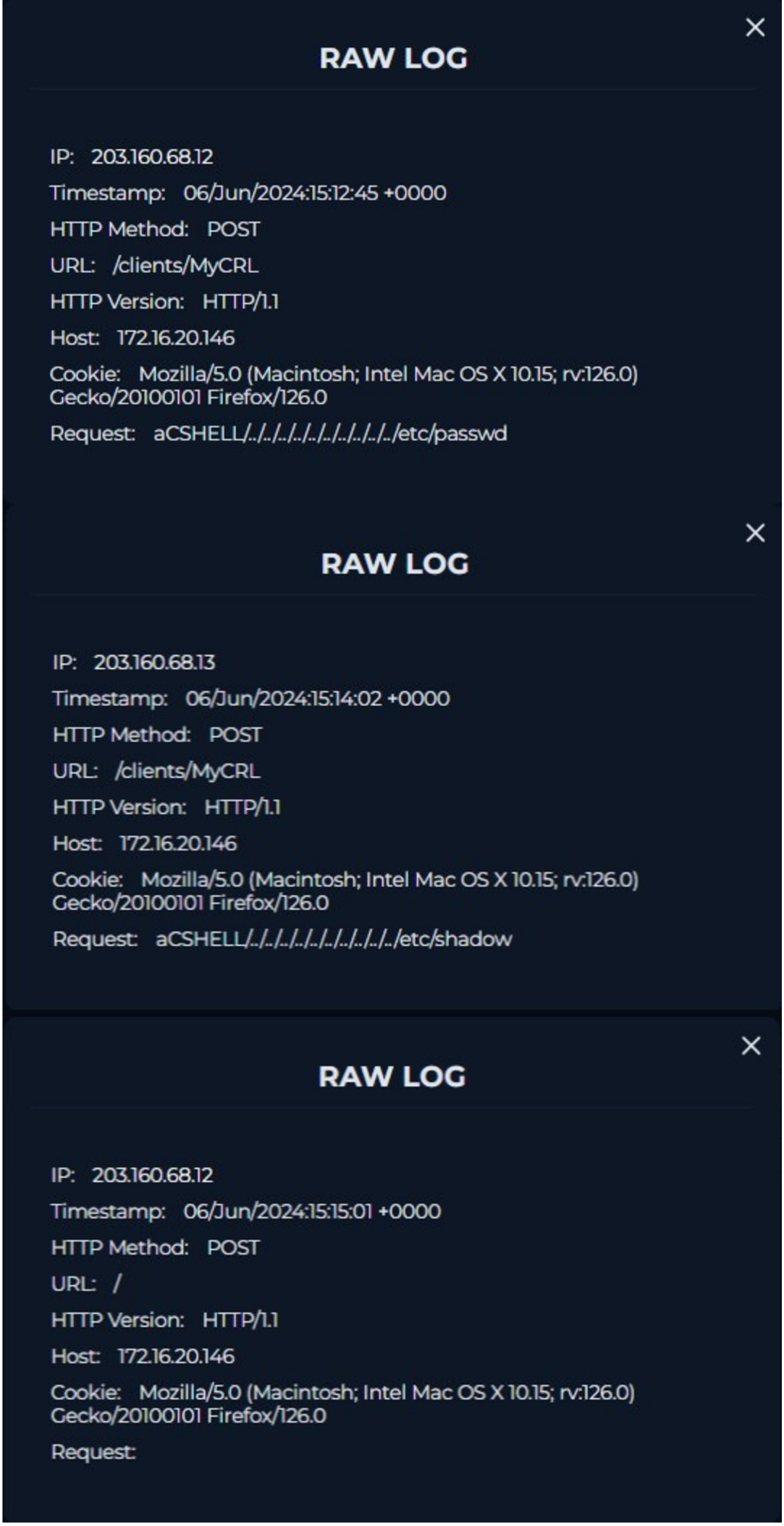
Reporter	IoA Timestamp (UTC)	Comment	Categories
NSCA-ISEU	2024-06-01 07:31:52 (1 year ago)	Check Point VPN Information Disclosure (CVE-2024-24919). VT: Malicious: 1 - Suspicious: 0. AS10099 ... show more	Port Scan, Web App Attack
Cyber SOC	2024-05-30 15:04:32 (1 year ago)	Peaksys - 2024-05-30 16:04:00 UTC+01	Port Scan

Step 3 — HTTP Traffic Inspection

Three key requests were identified around 03:12–03:15 PM:

Time	Method	Path	Response Code	Result
03:12 PM	GET	`/clients/MyCRL`	200	Information retrieved successfully (initial probing)
03:14 PM	POST	`/clients/MyCRL` → `/etc/passwd`	200	Successful read of passwd file
03:15 PM	POST	`/clients/MyCRL` → `/etc/shadow`	403	Access denied
03:15 PM	GET	`/`	512	Root access attempt failed

Observation:
The attacker was attempting to **enumerate and exfiltrate credential files**, confirming malicious intent.



Step 4 — Determine Attack Direction and Scope

- **Source:** Public IP (Internet).
- **Destination:** Internal gateway.
- **Scope:** Potential exposure of system accounts and hashes.
- No email vector found → attack not planned/phishing-based.

Step 5 — Endpoint Validation

- Confirmed that `CP-Spark-Gateway-01` executed `/etc/passwd` read request.
- Indicates **partial compromise** and possible credential exposure.
- Immediate **containment** required.

---

5. MITRE ATT&CK Mapping

Phase	Technique	ID	Description
Reconnaissance	Active Scanning	T1595.002	Scanning for vulnerable VPN and gateway services
Initial Access	Exploit Public-Facing Application	T1190	Exploiting Check Point Gateway path traversal vulnerability
Execution	Command and Scripting Interpreter	T1059	Shell-like command injection (`/aCSHELL/../../`) pattern
Discovery	File and Directory Discovery	T1083	Enumerating sensitive directories (`/etc/passwd`, `/etc/shadow`)
Collection	Data from Local System	T1005	Exfiltrating local files from target host

---

6. Actions Taken / Recommendations

1. **Containment:** Isolate`host CP-Spark-Gateway-01`immediately.
2. **Patch:** ApplyCheckPoint hotfix for CVE-2024-24919.
3. **Credential Hygiene:** Reset all admin and VPN credentials.
4. **Network Review:** Huntfor traffic from 203.160.68.12 across firewall and proxy logs.
5. **Threat Intel Enrichment:** Add source IP and domain `chinaunicom.cn` to deny list.
6. **Post-Incident:** Performforensic review of logs and system integrity checks.
7. **Awareness:** UpdateSOCplaybook to include detection rules for this CVE.

---

7. Analyst Conclusion

This incident was a **realexploitation attempt** of **CVE-2024-24919**, demonstrating an attacker leveraging **path traversal via HTTPS POST** to read sensitive Linux files on the Check Point Gateway.

The /etc/passwd file was successfully accessed, confirming a **partial breach**.
Containment and patching are critical to prevent further escalation and potential remote code execution.
