مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Critical Vulnerability in PaloAlto GlobalProtect

Tracking #:432315759

Date:15-04-2024

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed an actively exploited Critical OS command injection vulnerability impacting Palo Alto Networks Firewalls.

## TECHNICAL DETAILS:

**Vulnerability Details:**

- **CVE-2024-3400**
- **CVSS Score: 10.0 (Critical)**
- **Description**: OS command injection vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software.
- **Affected Products**: PAN-OS versions 10.2, 11.0, and 11.1 (specifically, when both GlobalProtect gateway and device telemetry are enabled).
- **Impact**: An unauthenticated attacker can potentially execute arbitrary code with root privileges on the target firewall.
- **Exploitation**: Limited in-the-wild exploitation confirmed by Palo Alto Networks.

**Fixed Versions:**

- **PAN-OS 10.2:**

- 10.2.9-h1 (Released 4/14/24)
- 10.2.8-h3 (ETA: 4/15/24)
- 10.2.7-h8 (ETA: 4/15/24)
- 10.2.6-h3 (ETA: 4/15/24)
- 10.2.5-h6 (ETA: 4/16/24)
- 10.2.3-h13 (ETA: 4/17/24)
- 10.2.1-h2 (ETA: 4/17/24)
- 10.2.2-h5 (ETA: 4/18/24)
- 10.2.0-h3 (ETA: 4/18/24)
- 10.2.4-h16 (ETA: 4/19/24)

- **PAN-OS 11.0:**

- 11.0.4-h1 (Released 4/14/24)
- 11.0.3-h10 (ETA: 4/15/24)
- 11.0.2-h4 (ETA: 4/16/24)
- 11.0.1-h4 (ETA: 4/17/24)
- 11.0.0-h3 (ETA: 4/18/24)

- **PAN-OS 11.1:**

- 11.1.2-h3 (Released 4/14/24)
- 11.1.1-h1 (ETA: 4/16/24)
- 11.1.0-h3 (ETA: 4/17/24)

- **Disable Device Telemetry (Temporary Mitigation)**: Palo Alto Networks recommends disabling device telemetry as a temporary mitigation step while awaiting the patch. Refer to Palo Alto Networks security advisory for specific instructions on how to do this. However, be aware that disabling device telemetry may impact certain PAN-OS functionalities

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Palo Alto Networks.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:


- https://security.paloaltonetworks.com/CVE-2024-3400