مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Exploited Vulnerability- Palo Alto Networks PAN-OS

Tracking #:432316678

Date:27-12-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical security vulnerability in Palo Alto Networks' PAN-OS software that is currently being exploited in the wild. This vulnerability could allow attackers to disrupt firewall operations, potentially leading to a denial-of-service (DoS) state on affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-3393**
- CVSS Score 8.7 High
- A critical security vulnerability in Palo Alto Networks' PAN-OS software that affects the DNS Security feature. This allows unauthenticated attackers to disrupt firewall operations and force them into maintenance mode.
- The vulnerability is triggered when a specially crafted malicious packet is sent through the firewall's data plane, causing the firewall to reboot and potentially enter a denial-of-service (DoS) state. Repeated exploitation attempts can force the firewall into maintenance mode

Exploitation in the Wild:

- Palo Alto Networks has confirmed instances where customers experienced DoS conditions due to their firewalls blocking malicious DNS packets exploiting this vulnerability.

Affected Versions:

- PAN-OS 11.2: Versions < 11.2.3
- PAN-OS 11.1: Versions < 11.1.5
- PAN-OS 10.2: Versions >= 10.2.8 and < 10.2.10-h12, < 10.2.13-h2
- PAN-OS 10.1: Versions >= 10.1.14 and < 10.1.14-h8
- Prisma Access: Versions >= 10.2.8 and < 11.2.3 on PAN-OS

PAN-OS 11.0, which has reached its end of life (EOL), will not receive a fix for this vulnerability

Fixed Versions:

- PAN-OS 10.1.14-h8
- PAN-OS 10.2.10-h12
- PAN-OS 11.1.5
- PAN-OS 11.2.3
- All later PAN-OS versions

Additional PAN-OS 11.1 fixes:

- 11.1.2-h16
- 11.1.3-h13
- 11.1.4-h7
- 11.1.5

Additional PAN-OS 10.2 fixes:

- 10.2.8-h19
- 10.2.9-h19
- 10.2.10-h12

- 10.2.11-h10
- 10.2.12-h4
- 10.2.13-h2
- 10.2.14

Additional PAN-OS 10.1 fixes:

- 10.1.14-h8
- 10.1.15

Additional PAN-OS fixes only applicable to Prisma Access:

- 10.2.9-h19
- 10.2.10-h12

Note: Refer to Palo Alto Networks advisory for workarounds and additional information.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided 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-2024-3393