مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Exploited Vulnerabilities in Palo Alto Networks PAN-OS

Tracking #:432316527

Date:19-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Palo Alto Networks has issued a security advisory addressing two actively exploited vulnerabilities affecting the management interface of PAN-OS.

TECHNICAL DETAILS:

Palo Alto Networks has issued a security advisory addressing two actively exploited vulnerabilities affecting the management interface of PAN-OS. These vulnerabilities, CVE-2024-0012 (Authentication Bypass) and CVE-2024-9474 (OS Command Injection), are being actively exploited in the wild. Both flaws reside in the management interface of PAN-OS, which could allow unauthenticated attackers to bypass authentication or execute arbitrary commands on vulnerable systems.

Vulnerability Details:

1. **CVE-2024-0012** PAN-OS: Authentication Bypass in the Management Web Interface
    - Severity 9.3, CRITICAL, **Urgency HIGHEST**
    - An authentication bypass in Palo Alto Networks PAN-OS software enables an unauthenticated attacker with network access to the management web interface to gain PAN-OS administrator privileges to perform administrative actions, tamper with the configuration, or exploit other authenticated privilege escalation vulnerabilities like CVE-2024-9474.

2. **CVE-2024-9474** PAN-OS: Privilege Escalation (PE) Vulnerability in the Web Management Interface
    - Severity 6.9, Medium, **Urgency HIGHEST**
    - A privilege escalation vulnerability in Palo Alto Networks PAN-OS software allows a PAN-OS administrator with access to the management web interface to perform actions on the firewall with root privileges.

Affected Products:

- PAN-OS 10.2, PAN-OS 11.0, PAN-OS 11.1, and PAN-OS 11.2 software.
- Cloud NGFW and Prisma Access are not impacted by this vulnerability.

Fixed Versions:

- PAN-OS 10.2.12-h2, PAN-OS 11.0.6-h1, PAN-OS 11.1.5-h1, PAN-OS 11.2.4-h1, and all later PAN-OS versions**.**

RECOMMENDATIONS:

- Ensure that all affected systems are updated to the patched versions as soon as possible.
- Restrict access to the PAN-OS management interface to trusted IP addresses or internal networks.
- Review system and firewall logs for signs of anomalous login attempts, unauthorized access, or unusual command execution that could indicate exploitation

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-2024-0012
- https://security.paloaltonetworks.com/CVE-2024-9474