مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Palo Alto Security Updates

Tracking #:432316382

Date:10-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Palo Alto has released security updates to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

Palo Alto Networks published security advisories to address vulnerabilities in multiple products.

1. **PAN-OS:**
   - CVE-2024-9468 PAN-OS: Firewall Denial of Service (DoS) via a Maliciously Crafted Packet- CVSSv4.0 Base Score: 8.2
   - Fixed Version- 10.2.9-h11, 10.2.10-h4, PAN-OS 10.2.11, PAN-OS 11.0.4-h5, PAN-OS 11.0.6, PAN-OS 11.1.3, and all later PAN-OS versions.

2. **Prisma Access Browser:**
   - PAN-SA-2024-0011 Chromium: Monthly Vulnerability Updates- CVSSv4.0 Base Score: 8.6
   - CVE-2024-8904, CVE-2024-8905, CVE-2024-8906, CVE-2024-8907, CVE-2024-8908, and CVE-2024-8909 are fixed in Prisma Access Browser 129.59.2896.5, and all later Prisma Access Browser versions.
   - CVE-2024-9120, CVE-2024-9121, CVE-2024-9122, and CVE-2024-9123 are fixed in Prisma Access Browser 129.71.2910.1, and all later Prisma Access Browser versions.
   - CVE-2024-7025, CVE-2024-9369, and CVE-2024-9370 are fixed in Prisma Access Browser 129.90.2910.2, and all later Prisma Access Browser versions.
   - CVE-2024-9602 and CVE-2024-9603 are fixed in Prisma Access Browser 129.101.2913.3, and all later Prisma Access Browser versions.

3. **Palo Alto Networks Expedition:**
   - CVE-2024-9463 (CVSS 9.9): An OS command injection vulnerability allowing an unauthenticated attacker to execute arbitrary OS commands as root, leading to the exposure of firewall usernames, passwords, and API keys.
   - CVE-2024-9464 (CVSS 9.3): A similar OS command injection vulnerability, but requiring authentication, allowing attackers to exploit Expedition and run OS commands as root.
   - CVE-2024-9465 (CVSS 9.2): An SQL injection vulnerability allowing unauthorized attackers to access Expedition's database, revealing password hashes, usernames, and more.
   - CVE-2024-9466 (CVSS 8.2): A cleartext storage vulnerability that exposes firewall usernames and passwords, posing a significant risk if not mitigated.
   - CVE-2024-9467 (CVSS 7.0): A reflected XSS vulnerability that allows attackers to execute malicious JavaScript via phishing attacks
   - The fixes for all listed issues are available in Expedition 1.2.96, and all later Expedition versions.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to apply the necessary updates 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