مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – Palo Alto

Tracking #:432316043

Date:11-07-2024

EXECUTIVE SUMMARY:

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

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-5910** | Base Score: 9.3 - Critical
  - Missing authentication for a critical function in Palo Alto Networks Expedition can lead to an Expedition admin account takeover for attackers with network access to Expedition.
  - Expedition is a tool aiding in configuration migration, tuning, and enrichment. Configuration secrets, credentials, and other data imported into Expedition is at risk due to this issue.

- **CVE-2024-5911** | Base Score: 7 - High
  - An arbitrary file upload vulnerability in Palo Alto Networks Panorama software enables an authenticated read-write administrator with access to the web interface to disrupt system processes and crash the Panorama.
  - Repeated attacks eventually cause the Panorama to enter maintenance mode, which requires manual intervention to bring the Panorama back online.

- **CVE-2024-5912** | Base Score: 6.8 - Medium
  - An improper file signature check in Palo Alto Networks Cortex XDR agent may allow an attacker to bypass the Cortex XDR agent's executable blocking capabilities and run untrusted executables on the device. This issue can be leveraged to execute untrusted software without being detected or blocked.

- **CVE-2024-5913 |** Base Score: 5.4 – Medium
  - An improper input validation vulnerability in Palo Alto Networks PAN-OS software enables an attacker with the ability to tamper with the physical file system to elevate privileges.

- **CVE-2024-3596 |** Base Score: 5.3 – Medium
  - This vulnerability allows an attacker performing a meddler-in-the-middle attack between Palo Alto Networks PAN-OS firewall and a RADIUS server to bypass authentication and escalate privileges to ‘superuser’ when RADIUS authentication is in use and either CHAP or PAP is selected in the RADIUS server profile.

Affected and versions and respective fixes:

Versions	Affected	Unaffected	CVE
Expedition 1.2	< 1.2.92	>= 1.2.92	CVE-2024-5910
PAN-OS 10.2	< 10.2.4 on Panorama	>= 10.2.4 on Panorama	CVE-2024-5911
PAN-OS 10.1	< 10.1.9 on Panorama	>= 10.1.9 on Panorama	CVE-2024-5911
Cortex XDR Agent 8.2	< 8.2.2	>= 8.2.2	CVE-2024-5912
Cortex XDR Agent 7.9-CE	< 7.9.102-CE	>= 7.9.102-CE	CVE-2024-5912
PAN-OS 11.2	< 11.2.1	>= 11.2.1	CVE-2024-5913
PAN-OS 11.1	< 11.1.4	>= 11.1.4	CVE-2024-5913
PAN-OS 11.0	< 11.0.5	>= 11.0.5	CVE-2024-5913
PAN-OS 10.2	< 10.2.10	>= 10.2.10	CVE-2024-5913
PAN-OS 10.1	< 10.1.14-h2	>= 10.1.14-h2	CVE-2024-5913
PAN-OS 11.1	< 11.1.3	>= 11.1.3	CVE-2024-3596
PAN-OS 11.0	< 11.0.4-h4	>= 11.0.4-h4	CVE-2024-3596
PAN-OS 10.2	< 10.2.10	>= 10.2.10	CVE-2024-3596
PAN-OS 10.1	< 10.1.14	>= 10.1.14	CVE-2024-3596
PAN-OS 9.1	< 9.1.19	>= 9.1.19	CVE-2024-3596
Prisma Access	All	None (Fix ETA: July 30)	CVE-2024-3596

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently 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-2024-5910
- https://security.paloaltonetworks.com/CVE-2024-5911
- https://security.paloaltonetworks.com/CVE-2024-5912
- https://security.paloaltonetworks.com/CVE-2024-5913
- https://security.paloaltonetworks.com/CVE-2024-3596