مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Palo Alto Security Updates

Tracking #:432316263

Date:12-09-2024

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 has published seven new security advisories and two informational bulletins on September 11, 2024 to address multiple vulnerabilities in its products.

1. **PAN-OS:**
   - CVE-2024-8686 PAN-OS: Command Injection Vulnerability (Severity: HIGH)
   - CVE-2024-8688 PAN-OS: Arbitrary File Read Vulnerability in the Command Line Interface (CLI) (Severity: MEDIUM)
   - CVE-2024-8691 PAN-OS: User Impersonation in GlobalProtect Portal (Severity: MEDIUM)

2. **Prisma Access Browser:**
   - PAN-SA-2024-0009- 8.6-(Severity: HIGH)-
   - Prisma Access Browser 128.138.2888.2 and later versions contain the fixes

3. **PAN-OS, GlobalProtect App, Prisma Access:**
   - CVE-2024-8687 PAN-OS: Cleartext Exposure of GlobalProtect Portal Passcodes (Severity: MEDIUM)

4. **ActiveMQ Content Pack:**
   - CVE-2024-8689 ActiveMQ Content Pack: Cleartext Exposure of Credentials (Severity: MEDIUM)

5. **Cortex XDR Agent:**
   - CVE-2024-8690 Cortex XDR Agent: Local Windows Administrator Can Disable the Agent (Severity: MEDIUM)

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/