مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Security Bulletin – Palo Alto Firewall

Tracking #:432316522

Date:18-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Palo Alto Networks has issued a critical security bulletin regarding a potential RCE vulnerability in firewall management interfaces.

TECHNICAL DETAILS:

Palo Alto Networks has reported an ongoing exploitation of an unauthenticated remote command execution (RCE) vulnerability affecting a limited number of firewall management interfaces exposed to the Internet. This vulnerability can potentially allow attackers to execute arbitrary commands on the affected devices without authentication, posing a significant security risk. Palo Alto Networks is urging all customers to immediately ensure that access to the management interfaces is restricted to trusted internal IP addresses only, in line with best practice deployment guidelines. Failure to properly secure these interfaces exposes organizations to the risk of full compromise of the firewall, which could lead to data breaches, unauthorized access, and network disruption.

Palo Alto Networks has released new indicators of compromise (IoCs) for the zero-day vulnerability impacting its PAN-OS firewall management interface has been actively exploited in the wild.
Raised the severity, Severity: CRITICAL

- CVSSv4.0 Base Score: 9.3
  (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L/E:A/AU:Y/R:U/V:C/RE:M/U:Red)

Indicators of compromise (IoCs):

- 136.144.17[.]*
- 173.239.218[.]251
- 216.73.162[.]*
- Note: these IP addresses may represent third party VPNs with legitimate user activity originating from these IPs to other destinations.
- Webshell with checksum 3C5F9034C86CB1952AA5BB07B4F77CE7D8BB5CC9FE5C029A32C72ADC7E814668.

RECOMMENDATIONS:

- Restrict Access to Management Interface: Ensure that access to the PAN-OS management interface is only possible from trusted internal IP addresses and is not accessible over the internet. This is in line with Palo Alto Networks' best practice deployment guidelines.
- Verify Device Configuration: Review current configuration and restrict any management interface access that may be exposed to untrusted networks, especially the internet. Follow Palo Alto Networks' security guidelines for managing and securing the management interface.
- Check for Exposed Devices: Log in to the Customer Support Portal and use the Assets section to identify devices that may have internet-facing management interfaces. Look for the tag PAN-SA-2024-0015 to identify these devices.

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/PAN-SA-2024-0015
- https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431