مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Security Bulletin- PAN-OS

Tracking #:432316496

Date:11-11-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Palo Alto Networks has issued an important informational bulletin regarding a potential vulnerability tied to the management interface of PAN-OS devices.

TECHNICAL DETAILS:

Palo Alto Networks has issued an important informational bulletin regarding a potential vulnerability tied to the management interface of PAN-OS devices. A claim of a remote code execution vulnerability has been identified externally, but details of the issue are currently unknown. As a precautionary measure, Palo Alto Networks strongly advises customers to ensure their management interfaces are secured in accordance with industry best practices.
The vulnerability could expose devices whose management interfaces are not properly restricted to trusted internal IPs, increasing the risk of unauthorized access and potential exploitation. While no exploitation has been observed to date, Palo Alto Networks is actively monitoring the situation and recommends immediate action to secure any affected devices.

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.
- Stay Updated on Exploitation Status: Although no exploitation has been observed, it is essential to stay informed about any potential developments. Subscribe to Palo Alto Networks' RSS feed or email notifications to receive real-time updates on this issue.
- Review Further Guidance: Palo Alto Networks has provided detailed instructions on securing the management interface.

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