Critical Vulnerability Alert

15 November 2024

TLP: AMBER
No third party distribution
Tags: Initial Access, Technology Stack-Related: Firewall, Security Solutions

Actively Exploited Unauthenticated Remote Command Execution Vulnerability in Palo Alto Firewall Management Interfaces (PAN-SA-2024-0015)

Introduction

On 15 November 2024, Palo Alto Networks updated the Security Advisory, raising the severity of this bulletin due to observed threat activity impacting the devices whose access to the Firewall Management Interface by Palo Alto Network. [1] The `PAN-SA-2024-0015` vulnerability enables a remote, unauthenticated attacker to achieve remote code execution (RCE) via the PAN-OS management interface. Palo Alto Networks has observed threat activity exploiting an unauthenticated remote command execution vulnerability against a limited number of firewall management interfaces which are exposed to the Internet.[2] As of the time of writing, despite no exploitation information being found in the security advisory, Palo Alto Networks is actively investigating this activity.[3] **PwC's Dark Lab will keep monitoring and continue to update this advisory as new information becomes available.**

PwC's Dark Lab urges impacted clients to follow Palo Alto Networks' security advisory[4] immediately to secure the management access of your Palo Alto Networks device, given the active exploitation in the wild. The following report is issued as it satisfies our criteria for the release of a critical vulnerability alert.

PwC's Dark Lab summarises the known information regarding this vulnerability below:

CVE(s)	`TBD`
CVE Published Date	15 November 2024
CVSS v3	NVD score not yet assigned, vendor assigned 9.3[5]
Potentially Affected Products	• Devices whose access to the Management Interface by Palo Alto Networks except: * ○ Prisma Access ○ Cloud Next Generation Firewalls (NGFWs) *Please refer to "Required Configuration for Exposure" to identify any devices with internet-facing management interface for your account.
Description	Unauthenticated Remote Command Execution Vulnerability in Palo Alto Firewall Management Interfaces
Potential Impact	Remote Code Execution

[1] https://security.paloaltonetworks.com/PAN-SA-2024-0015
[2] https://security.paloaltonetworks.com/PAN-SA-2024-0015
[3] https://security.paloaltonetworks.com/PAN-SA-2024-0015
[4] https://security.paloaltonetworks.com/PAN-SA-2024-0015
[5] https://security.paloaltonetworks.com/PAN-SA-2024-0015

Proof of Concept (PoC) Available	No
Exploited in the Wild	Yes[6]
Patch Available	No
Workaround Available	Yes[7]

Impact and Analysis

The `PAN-SA-2024-0015` vulnerability is a critical RCE Vulnerability identified in devices by Palo Alto Networks whose access to Firewall Management Interface. Palo Alto Networks has not disclosed specific technical details regarding the mechanics of the vulnerability or the precise conditions under which it can be exploited.[8]

Palo Alto Networks has observed threat activity exploiting an unauthenticated remote command execution vulnerability against a limited number of firewall management interfaces which are exposed to the Internet.[9] As of the time of writing, there are no known instances of exploitation, or indicators of compromise (IOCs) related to the `PAN-SA-2024-0015` vulnerability.

It is important to note that **neither Prisma Access nor cloud NGFW is affected by this vulnerability.[10]**

Detection

Required Configuration for Exposure

At this time, Palo Alto Networks believe devices whose access to the Management Interface is not secured.[11]

Steps to identify your devices:

Step 1. To find your assets that require remediation action visit the Assets section of Customer Support Portal at https://support.paloaltonetworks.com (Products → Assets → All Assets → Remediation Required).

Step 2. The list of your devices with an internet-facing management interface discovered in the scans are tagged with `PAN-SA-2024-0015`. If no such devices are listed, it indicates the scan did not find any devices with internet-facing management interface for your account.

[6] https://security.paloaltonetworks.com/PAN-SA-2024-0015
[7] https://security.paloaltonetworks.com/PAN-SA-2024-0015
[8] https://security.paloaltonetworks.com/PAN-SA-2024-0015
[9] https://security.paloaltonetworks.com/PAN-SA-2024-0015
[10] https://security.paloaltonetworks.com/PAN-SA-2024-0015
[11] https://security.paloaltonetworks.com/PAN-SA-2024-0015

Mitigation

Palo Alto Networks recommends that customers ensure their management interface is configured according to best practices. This includes:[12]

- **Restricting access to trusted internal IPs**
- **Ensuring that the management interface is not accessible from the Internet**

For further guidance, Palo Alto Networks provides a resource on securing management access, which can be found here: How to Secure the Management Access of Your Palo Alto Networks Device[13]. Organizations are encouraged to implement these recommendations immediately to mitigate potential risks associated with the `PAN-SA-2024-0015` vulnerability.

Conclusion

Given the active exploitation of the `PAN-SA-2024-0015` vulnerability, we strongly urge impacted clients to follow the advisory issued by Palo Alto Networks immediately. Although there are currently a limited number of exploits and no known instances of exploitation by threat actor groups[14], the remote unauthenticated nature of this vulnerability poses a high risk for exploitation. Such firewall-related vulnerabilities can have severe impacts, if exploited. Prompt action is strongly recommended to mitigate potential exploitation attempts.

Further information

If you need any further advice or would like PwC's leading global incident response team to support you, please do not hesitate to contact us.

This report has been provided to clients as part of PwC's Dark Lab Cyber-as-a-Service offering. More detailed analysis on the topics covered in this report can be provided on request.

If you would like more information on any of the threats discussed in this alert, please feel free to get in touch, by emailing *darklab.cti@hk.pwc.com*.

Traffic Light Protocol

This report is classified as TLP: AMBER. Recipients may only share TLP: AMBER information with members of their own organisation who need to know the information to protect themselves or prevent further harm.

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

This document has been prepared by PricewaterhouseCoopers Limited (PwC) solely for its clients who have entered into a subscription agreement with PwC for related services (the "subscription") and solely for the purpose and on the terms set out in the subscription. PwC accepts no liability (including for negligence) to anyone else in connection with this document. It may only be distributed according to the TLP classification where one is provided, and otherwise it may not be provided to anyone else.