

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

CVE-2025-0108: PAN-OS Authentication Bypass Flaw Under Active Exploitation

Date of Publication

February 17, 2025

Admiralty Code

A1

TA Number

TA2025043




Summary

First Seen: February 12, 2024

Affected Product: Palo Alto Networks PAN-OS

Impact: CVE-2025-0108 is a high-severity authentication bypass vulnerability in Palo Alto Networks' PAN-OS, allowing unauthenticated attackers to exploit inconsistencies in the management web interface (Nginx, Apache, PHP). While it does not enable remote code execution, it compromises system integrity. Palo Alto Networks has released patches, and active exploitation has been observed since the PoC became available on February 13, 2025. Organizations should update immediately and restrict management access to trusted IPs to mitigate risks.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-0108	Palo Alto Networks PAN-OS Management Interface Authentication Bypass Vulnerability	Palo Alto Networks PAN-OS			

Vulnerability Details

#1

CVE-2025-0108 is a high-severity authentication bypass vulnerability affecting Palo Alto Networks' PAN-OS software. This flaw allows unauthenticated attackers with network access to the management web interface to bypass authentication and invoke specific PHP scripts. While this does not permit remote code execution, it can compromise the integrity and confidentiality of the system.

#2

The vulnerability arises from discrepancies in how the management interface's components Nginx, Apache, and the PHP application process web requests. Attackers can craft specially designed HTTP requests to exploit these inconsistencies, effectively bypassing authentication mechanisms.

#3

Palo Alto Networks has released patches to address this issue in PAN-OS versions 11.2.4-h4, 11.1.6-h1, 10.2.13-h3, and 10.1.14-h9. In addition to applying patches, it is crucial to restrict access to the management web interface to trusted internal IP addresses, significantly reducing the risk of unauthorized exploitation.

#4

Researchers discovered CVE-2025-0108 while analyzing patches for prior PAN-OS vulnerabilities, [CVE-2024-0012](#) and [CVE-2024-9474](#). Active exploitation attempts have been observed, with attacks originating from multiple IP addresses beginning on February 13, 2025. Given that proof-of-concept (PoC) exploit code is publicly available, it is likely that exploitation efforts by various threat actors will increase.

#5

Organizations using vulnerable PAN-OS versions should prioritize updating their systems and implementing recommended security measures to mitigate potential risks.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-0108	PAN-OS 10.1 versions earlier than 10.1.14-h9 PAN-OS 10.2 versions earlier than 10.2.13-h3 PAN-OS 11.1 versions earlier than 11.1.6-h1 PAN-OS 11.2 versions earlier than 11.2.4-h4 PAN-OS 11.0 (EOL)	cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*	CWE-306

Recommendations



Apply Patches Immediately: Apply the latest patches provided by Palo Alto Networks to eliminate the vulnerability. Fixed versions include: 11.2.4-h4 and later, 11.1.6-h1 and later, 10.2.13-h3 and later, 10.1.14-h9 and later. If an immediate upgrade is not possible, implement mitigation measures to reduce exposure.



Restrict Access to Management Interface: Block external access by limiting access to the management web interface to only trusted internal IP addresses using firewalls, VPN access controls, or Zero Trust Network Architecture (ZTNA). Disable unnecessary access if remote management is not required.



Implement Network Security Controls: Monitor network traffic using intrusion detection/prevention systems (IDS/IPS) to detect suspicious activity targeting CVE-2025-0108. Use geo-blocking to restrict access from high-risk regions if applicable. Enable logging to detect unauthorized login attempts and exploit attempts.



Network Segmentation: Place management interfaces on separate, secure networks that are not accessible from the public internet.



Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0002</u> Execution	<u>TA0004</u> Privilege Escalation	<u>TA0001</u> Initial Access
<u>T1203</u> Exploitation for Client Execution	<u>T1068</u> Exploitation for Privilege Escalation	<u>T1190</u> Exploit Public-Facing Application	<u>T1588.006</u> Vulnerabilities
<u>T1588</u> Obtain Capabilities	<u>T1588.005</u> Exploits		

✂ Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	198[.]23[.]171[.]159, 43[.]159[.]135[.]197, 38[.]54[.]50[.]252, 38[.]54[.]101[.]65, 1[.]55[.]112[.]205, 84[.]17[.]43[.]35, 43[.]157[.]45[.]216, 85[.]31[.]231[.]183, 46[.]246[.]9[.]213, 194[.]233[.]96[.]86

Patch Details

Upgrade Palo Alto Networks PAN-OS to the following versions:

- 11.2.4-h4 and later
- 11.1.6-h1 and later
- 10.2.13-h3 and later
- 10.1.14-h9 and later

Note: PAN-OS 11.0 is End-of-Life (EOL). If using this version, upgrade to a supported release immediately.

Link:

<https://security.paloaltonetworks.com/CVE-2025-0108>

References

<https://slcyber.io/blog/nginx-apache-path-confusion-to-auth-bypass-in-pan-os/>

https://socradar.io/palo-alto-firewall-vulnerability-cve-2025-0108-exploit/?utm_source=feedly

<https://github.com/iSee857/CVE-2025-0108-PoC>

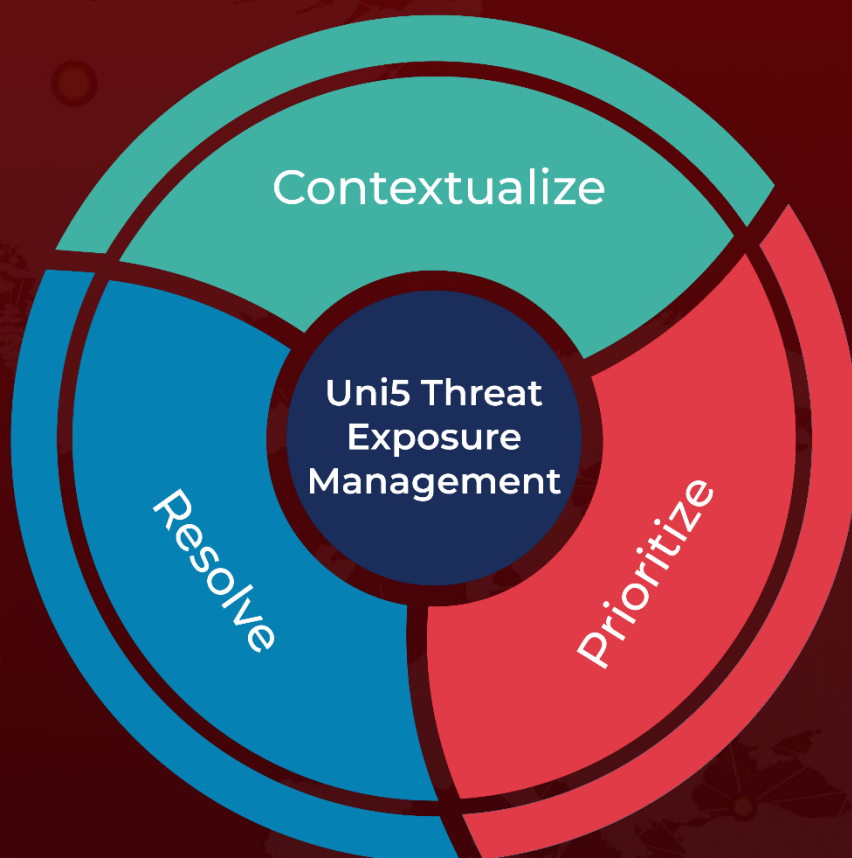
<https://www.greynoise.io/blog/greynoise-observes-active-exploitation-of-pan-os-authentication-bypass-vulnerability-cve-2025-0108>

<https://hivepro.com/threat-advisory/critical-zero-day-pan-os-flaws-exposing-systems-to-full-control/>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

February 17, 2025 • 4:30 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com