NATIONAL CSIRT-CY

CVE-2025-0108

19/02/2025

Authentication Bypass in the Management Web Interface

CONFIDENTIAL

Executive Summary

An authentication bypass in the Palo Alto Networks PAN-OS software enables an unauthenticated attacker with network access to the management web interface to bypass the authentication otherwise required by the PAN-OS management web interface and invoke certain PHP scripts. While invoking these PHP scripts does not enable remote code execution, it can negatively impact integrity and confidentiality of PAN-OS

https://securityadvisories.paloaltonetworks.com/CVE-2025-0108

Analysis

The risk is greatest if you enabled access to the management interface from the internet or any untrusted network either:

- Directly or
- Through a dataplane interface that includes a management interface profile.

You greatly reduce the risk if you ensure that you allow only trusted internal IP addresses to access the management interface.

Palo Alto Networks has observed exploit attempts chaining CVE-2025-0108 with CVE-2024-9474 and CVE-2025-0111 on unpatched and unsecured PAN-OS web management interfaces.

Common Weakness Enumeration

https://cwe.mitre.org/data/definitions/306.html

Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/CVE-2025-0108

Affected Systems

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 11.2	< 11.2.4-h4	>= 11.2.4-h4
PAN-OS 11.1	< 11.1.6-h1	>= 11.1.6-h1
PAN-OS 10.2	< 10.2.7-h24 < 10.2.8-h21 < 10.2.9-h21 < 10.2.12-h6 < 10.2.13-h3	>= 10.2.7-h24 >= 10.2.8-h21 >= 10.2.9-h21 >= 10.2.12-h6 >= 10.2.13-h3
PAN-OS 10.1	< 10.1.14-h9	>= 10.1.14-h9
Prisma Access	None	All

Solutions

Version	Minor Version	Suggested Solution
PAN-OS 10.1	10.1.0 through 10.1.14	Upgrade to 10.1.14-h9 or later
PAN-OS 10.2	10.2.0 through 10.2.13	Upgrade to 10.2.13-h3 or later
	10.2.7	Upgrade to 10.2.7-h24 or 10.2.13-h3 or later
	10.2.8	Upgrade to 10.2.8-h21 or 10.2.13-h3 or later
	10.2.9	Upgrade to 10.2.9-h21 or 10.2.13-h3 or later
	10.2.12	Upgrade to 10.2.12-h6 or 10.2.13-h3 or later
PAN-OS 11.0 (EoL)		Upgrade to a supported fixed version
PAN-OS 11.1	11.1.0 through 11.1.6	Upgrade to 11.1.6-h1 or later
PAN-OS 11.2	11.2.0 through 11.2.4	Upgrade to 11.2.4-h4 or later

Note: PAN-OS 11.0 reached end of life (EoL) on November 17, 2024. No additional fixes are planned for this release.

Mitigations

Restrict management interface access to only trusted internal IP addresses.

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.