An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

NCSC #2502190163

NCSC Advisory

A Critical Vulnerability Exists in Palo Alto Networks PAN-OS Software CVE-2025-0108

19th, February 2025

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use **TLP:CLEAR** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2025-0108

Published: 2025-02-12

Vendor: Palo Alto Networks

Product: PAN-OS

CVSS Score[1]: 8.8

Products Affected

Version	Affected
PAN-OS 11.2	< 11.2.4-h4
PAN-OS 11.1	< 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
PAN-OS 10.1	< 10.1.14-h9

Impact

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.

You can greatly reduce the risk of this issue by restricting access to the management web interface to only trusted internal IP addresses according to Palo Altos recommended best practices deployment guidelines found here.

This issue does not affect Cloud NGFW or Prisma Access software.

[1] https://www.first.org/cvss/v4.0/specification-document

Common Weakness Enumeration (CWE)[2]: CWE-306: Missing Authentication for Critical Function

Known Exploited Vulnerability (KEV) catalog[3]: Yes

Used by Ransomware Operators: N/A

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Palo Alto Networks.

- https://nvd.nist.gov/vuln/detail/CVE-2025-0108
- https://www.cve.org/CVERecord?id=CVE-2025-0108
- https://security.paloaltonetworks.com/CVE-2025-0108