An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2411190160

NCSC Advisory

Authentication Bypass in the Management Web Interface, Palo Alto Networks PAN-OS (CVE-2024-0012) - CVSSv3: 9.3

21st November 2024

Update v1.1

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.

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

Revision History

Revision	Date	Author(s)	Description
1.0	19th October 2024	CSIRT-IE	Initial Advisory
1.1	21st November 2024	CSIRT-IE	Updated advisory

Description

CVE ID: CVE-2024-0012

Published: 2024-11-18

Vendor: Palo Alto Networks

Product: PAN-OS

CVSS3.0 Score[1]: 9.3

Products Affected

Versions	Affected
PAN-OS 11.2	versions less than 11.2.4-h1
PAN-OS 11.1	versions less than 11.1.5-h1
PAN-OS 11.0	versions less than 11.0.6-h1
PAN-OS 10.2	versions less than 10.2.12-h2

Impact

An authentication bypass in Palo Alto Networks PAN-OS software enables an unauthenticated attacker with network access to the management web interface to gain PAN-OS administrator privileges to perform administrative actions, tamper with the configuration, or exploit other authenticated privilege escalation vulnerabilities like CVE-2024-9474[2].

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://security.paloaltonetworks.com/CVE-2024-9474

The risk of this issue is greatly reduced if you secure access to the management web interface by restricting access to only trusted internal IP addresses according to the Palo Alto recommended best practice deployment guidelines, linked below.

This issue is applicable only to PAN-OS 10.2, PAN-OS 11.0, PAN-OS 11.1, and PAN-OS 11.2 software. Cloud NGFW and Prisma Access **are not impacted** by this vulnerability.

Common Weakness Enumeration (CWE)[3]: CWE-306 Missing Authentication for Critical Function

Known Exploited Vulnerability (KEV) catalog[4]: No

Used by Ransomware Operators: N/A

Recommedations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from Palo Alto Networks:

- https://security.paloaltonetworks.com/CVE-2024-0012
- https://security.paloaltonetworks.com/CVE-2024-9474
- https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431

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

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