An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2411110171

NCSC Advisory

Critical vulnerability exists in Palo Alto Networks Expedition: CVE-2024-5910 (CVSSv3: 9.3)

Day 11th, November 2024

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

Description

CVE ID: CVE-2024-5910

Published: 2024-07-10T19:15:00

Vendor: Palo Alto Networks

Product: Expedition

CVSS3.0 Score[1]: 9.3

Summary:
Missing authentication for a critical function in Palo Alto Networks Expedition can lead to an Expedition admin account takeover for attackers with network access to Expedition.

Note: Expedition is a tool aiding in configuration migration, tuning, and enrichment. Configuration secrets, credentials, and other data imported into Expedition is at risk due to this issue.

Palo Alto Networks is aware of reports from CISA that there is evidence of active exploitation for this CVE.

Products affected

- Palo Alto Networks Expedition 1.2 prior to version 1.2.92

Impact

Exploitation can lead to an Expedition admin account takeover for attackers with network access to Expedition.

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

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

Used by Ransomware Operators: Known

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://cwe.mitre.org/
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly advises affected organisations to ensure networks access to Expedition is restricted to authorised users, hosts, or networks. Please also review the latest release notes and install the relevant updates from Palo Alto Networks.

Additional recommendations and mitigations for CVE-2024-5910 can be found in the respective link(s) below:

https://security.paloaltonetworks.com/CVE-2024-5910