National Cyber Security Centre

[2408190142]-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerability exists in Palo Alto Networks Cortex XSOAR CommonScripts (CVE-2024-5914)

Monday 19th August, 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.

Description

Published: 2024-08-14T17:15:00
Vendor: Palo Alto Networks
Product: Cortex XSOAR CommonScripts
CVE ID: CVE-2024-5914
CVSS 4.0 Score[1]**:** 7.0
EPSS[2]**:** 0.095050000 - For up to date EPSS Score Click here: https://api.first.org/data/v1/epss?cve=CVE-2024-5914

Summary: A command injection issue in Palo Alto Networks Cortex XSOAR CommonScripts Pack allows an unauthenticated attacker to execute arbitrary commands within the context of an integration container.

More information related to this issue can be found at the following link(s):
https://security.paloaltonetworks.com/CVE-2024-5914

Products Affected

- Palo Alto Networks Cortex XSOAR CommonScripts all versions prior to 1.12.33

  To be exposed, an integration must make use of the ScheduleGenericPolling or GenericPollingScheduledTask scripts from the CommonScripts pack.

Impact

Common Weakness Enumeration (CWE)[3]**:** CWE-77 Improper Neutralization of Special Elements used in a Command (’Command Injection’)

Present in CISA Known Exploited Vulnerability(KEV)[4] **catalog:** NO

Recommendations

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

Additional recommendations and mitigation’s for CVE-2024-5914 can be found in the respective link(s) below:

https://security.paloaltonetworks.com/CVE-2024-5914

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

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
Tom Johnson House,
Beggars Bush,
Dublin, D04 A068,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre