Security Advisory 2024-083

Palo Alto Cortex XSOAR CommonScripts Critical Vulnerability

August 20, 2024 — v1.1

TLP:CLEAR

History:

- *19/08/2024 — v1.0 – Initial publication*
- *20/08/2024 — v1.1 – Correction to specify that only CommonScripts Pack is affected*

Summary

On August 14, 2024, Palo Alto Networks released a security advisory for a critical command injection vulnerability, **CVE-2024-5914**, in Cortex XSOAR [1, 2]. This flaw allows unauthenticated attackers to execute arbitrary commands within the context of an integration container, potentially compromising the system. The vulnerability affects the product's CommonScripts Pack and is rated as high severity with a CVSS score of 9.0.

Technical Details

CVE-2024-5914 is a command injection vulnerability that can be exploited without authentication. It affects specific configurations of Cortex XSOAR's CommonScripts Pack, allowing remote attackers to execute arbitrary commands.

Affected Products

- Palo Alto Networks Cortex XSOAR CommonScripts prior to 1.12.33 [2]

Recommendations

CERT-EU recommends applying the patches included in versions starting with 1.12.33 immediately to mitigate this vulnerability.

References

[1] https://www.securityweek.com/palo-alto-networks-patches-unauthenticated-command-execution-flaw-in-cortex-xsoar/

[2] https://security.paloaltonetworks.com/CVE-2024-5914