



Advisory Alert

Alert Number: AAA20231110

Date: November 10, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Palo Alto	Medium	Local Privilege Escalation

Description

Affected Product	Palo Alto
Severity	Medium
Affected Vulnerability	Local Privilege Escalation (CVE-2023-3282)
Description	<p>Palo Alto has released a security update addressing a local privilege escalation vulnerability in the Cortex XSOAR engine software running on a Linux operating system that enables a local attacker to execute programs with elevated privileges if the attacker has shell access to the engine.</p> <p>Palo Alto recommends to apply the necessary patch updates at your earliest to avoid issues.</p>
Affected Products	Cortex XSOAR 6.10 to 6.10.0.250144 on Linux
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2023-3282

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.

Financial Sector Computer Security Incident Response Team (FinCSIRT)

LankaPay Pvt Ltd, Level 18, Bank of Ceylon Head Office, BOC Square, 01 Bank of Ceylon Mawatha, Colombo 00100, Sri Lanka

Hotline: + 94 112039777