Palo Alto Networks Cortex XSOAR/XSIAM CommvaultSecurityIQ Vulnerability

Severity Level: High

Components Affected

- Cortex XSOAR CommvaultSecurityIQ Marketplace integration versions prior to 1.2.0
- Cortex XSIAM CommvaultSecurityIQ Marketplace integration versions prior to 1.2.0

Overview

A security vulnerability has been identified in Palo Alto Networks Cortex XSOAR and Cortex XSIAM CommvaultSecurityIQ integration. The vulnerability could allow an attacker with network access to bypass expected security validation mechanisms and interact with protected resources.

Successful exploitation of this vulnerability may result in unauthorized access to sensitive security automation functions, exposure of confidential information, and potential manipulation of integrated security operations workflows.

Description

A vulnerability has been discovered in Palo Alto Networks Cortex XSOAR and Cortex XSIAM CommvaultSecurityIQ integration, the most severe of which could allow unauthorized access to protected resources. Details of the vulnerability are as follows:

- An attacker may be able to bypass authentication validation and access protected resources without proper authorization. (CVE-2026-0274)
- An attacker may be able to interact with integrated security automation functions using invalid or improperly validated credentials. (CVE-2026-0274)
- Successful exploitation may allow unauthorized users to view sensitive information, modify configurations, or perform actions within connected security environments. (CVE-2026-0274)

Impact

- Unauthorized Access
- Information Disclosure
- Data Manipulation
- Privilege Misuse
- Security Control Bypass

Solution/ Workarounds

Before installation of the software, please visit the vendor web-site for more details.

Apply fixes issued by the vendor:

- Upgrade Cortex XSOAR CommvaultSecurityIQ Marketplace integration to version 1.2.0 or later.
- Upgrade Cortex XSIAM CommvaultSecurityIQ Marketplace integration to version 1.2.0 or later.

Reference

- https://security.paloaltonetworks.com/CVE-2026-0274
- https://www.tenable.com/cve/CVE-2026-0274

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.