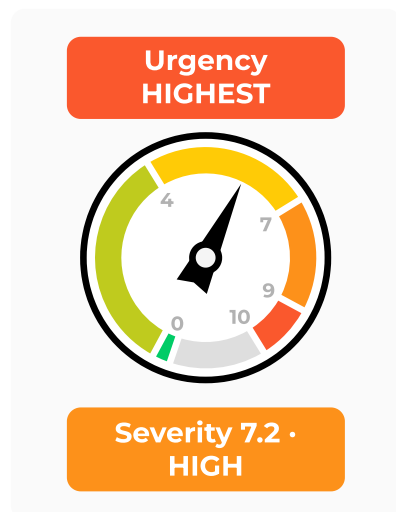


Palo Alto Networks Security Advisories / CVE-2026-0234

## CVE-2026-0234 Cortex XSOAR: Improper Verification of Cryptographic Signature in Microsoft Teams integration



Exploit Maturity <b>UNREPORTED</b>	Response Effort <b>MODERATE</b>	Recovery <b>USER</b>	Value Density <b>DIFFUSE</b>
Attack Vector <b>NETWORK</b>	Attack Complexity <b>HIGH</b>	Attack Requirements <b>PRESENT</b>	Automatable <b>NO</b>
User Interaction <b>NONE</b>	Product Confidentiality <b>HIGH</b>	Product Integrity <b>HIGH</b>	Product Availability <b>HIGH</b>
Privileges Required <b>NONE</b>	Subsequent Confidentiality <b>NONE</b>	Subsequent Integrity <b>NONE</b>	Subsequent Availability <b>NONE</b>

[CVE](#)
[JSON](#)
[CSAF](#)

 Published

**2026-04-08**
 Updated

**2026-04-08**

Discovered

**externally**

### Description

An improper verification of cryptographic signature vulnerability exists in Cortex XSOAR and Cortex XSIAM platforms during integration of Microsoft Teams that enables an unauthenticated user to access and modify protected resources.

### Product Status

Versions	Affected	Unaffected
Cortex XSIAM Microsoft Teams Marketplace 1.5.0	< 1.5.52	>= 1.5.52
Cortex XSOAR Microsoft Teams Marketplace 1.5.0	< 1.5.52	>= 1.5.52

**Severity: HIGH, Suggested Urgency: HIGHEST**

CVSS-BT: 7.2 / CVSS-B: 9.2

(CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/AU:N/R:U/V:D/RE:M/U:Red)

## Exploitation Status

---

Palo Alto Networks is not aware of any malicious exploitation of this issue.

## Weakness Type and Impact

---

CWE-347 Improper Verification of Cryptographic Signature

CAPEC-475 Signature Spoofing by Improper Validation

## Solution

---

Version	Minor Version	Suggested Solution
Cortex XSOAR Microsoft Teams Marketplace 1.5	1.5.0 through 1.5.51	Upgrade to 1.5.52 or later.
Cortex XSIAM Microsoft Teams Marketplace 1.5	1.5.0 through 1.5.51	Upgrade to 1.5.52 or later.

## Workarounds and Mitigations

---

No known workarounds exist for this issue.

## Acknowledgments

---



Palo Alto Networks thanks quinn for discovering and reporting this issue.

## CPE Applicability

---

- ○ cpe:2.3:a:palo\_alto\_networks:cortex\_xsoar\_microsoft\_teams\_marketplace:\*\*\*\*\* is vulnerable from (including)1.5.0 and up to (excluding)1.5.52
- or
- ○ cpe:2.3:a:palo\_alto\_networks:cortex\_xsiam\_microsoft\_teams\_marketplace:\*\*\*\*\* is vulnerable from (including)1.5.0 and up to (excluding)1.5.52

## Timeline

---

2026-04-08 ○ Initial Publication

© 2026 Palo Alto Networks, Inc. All rights reserved.