Cortex XSOAR: Improper Verification of Cryptographic Signature in Microsoft Teams integration

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-0234
State	PUBLISHED
Assigner	palo_alto
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-13 08:16:22 UTC
Updated	2026-04-13 15:01:43 UTC
Description	An improper verification of cryptographic signature vulnerability exists in Cortex XSOAR and Cortex XSIAM platforms during

Risk And Classification

Primary CVSS: v4.0 7.2 HIGH from psirt@paloaltonetworks.com

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/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:N/R:U/V:D/RE:M/U:Red

EPSS: 0.000270000 probability, percentile 0.073670000 (date 2026-04-15)

Problem Types: CWE-347 | CWE-347 CWE-347 Improper Verification of Cryptographic Signature

Version	Source	Type	Score	Severity	Vector
4.0	psirt@paloaltonetworks.com	Secondary	7.2	HIGH	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/S
4.0	CNA	CVSS	7.2	HIGH	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:N/R:U/V:D/RE:M/U:Red

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Palo Alto Networks	Cortex XSOAR Microsoft Teams Marketplace	affected 1.5.0 1.5.52 custom	Not specified
CNA	Palo Alto Networks	Cortex XSIAM Microsoft Teams Marketplace	affected 1.5.0 1.5.52 custom	Not specified

References

Reference	Source	Link	Tags
security.paloaltonetworks.com/CVE-2026-0234	psirt@paloaltonetworks.com	security.paloaltonetworks.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: quinn (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-04-08T16:00:00.000Z	Initial Publication

Solutions

CNA: 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

CNA: No known workarounds exist for this issue.

Exploits

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

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**