Cortex XDR Agent: Local Administrator can disable the agent on Windows

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

Summary

CVE	CVE-2026-0232
State	PUBLISHED
Assigner	palo_alto
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-13 08:16:20 UTC
Updated	2026-04-13 15:01:43 UTC
Description	A problem with a protection mechanism in the Palo Alto Networks Cortex XDR agent on Windows allows a local Windows a

Risk And Classification

Primary CVSS: v4.0 4 MEDIUM from psirt@paloaltonetworks.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:N/VI:N/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:Y/R:U/V:D/RE:M/U:Amber

EPSS: 0.000130000 probability, percentile 0.021130000 (date 2026-04-15)

Problem Types: CWE-15 | CWE-15 CWE-15: External Control of System or Configuration Setting

Version	Source	Type	Score	Severity	Vector
4.0	psirt@paloaltonetworks.com	Secondary	4	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/S
4.0	CNA	CVSS	4	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/S

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:N/VI:N/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:Y/R:U/V:D/RE:M/U:Amber

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Palo Alto Networks	Cortex XDR Agent	unaffected 9.1.0 5.10.14 custom	Not specified
CNA	Palo Alto Networks	Cortex XDR Agent	unaffected 9.0 custom	Not specified
CNA	Palo Alto Networks	Cortex XDR Agent	unaffected 8.9 custom	Not specified
CNA	Palo Alto Networks	Cortex XDR Agent	unaffected 8.7-CE custom	Not specified
CNA	Palo Alto Networks	Cortex XDR Agent	affected 9.0 9.0.1 custom	Windows
CNA	Palo Alto Networks	Cortex XDR Agent	affected 8.9 8.9.1 custom	Windows
CNA	Palo Alto Networks	Cortex XDR Agent	affected 8.7-CE 8.7.101-CE custom	Windows
CNA	Palo Alto Networks	Cortex XDR Agent	affected 8.3-CE 8.3-CE-CU-2120 custom	Windows
CNA	Palo Alto Networks	Cortex XDR Agent	affected 7.9-CE 7.9-CE-CU-2120 custom	Windows

References

Reference	Source	Link	Tags
security.paloaltonetworks.com/CVE-2026-0232	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: WhatThe0xDoin (en)

Additional Advisory Data

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

Solutions

CNA: To fully remediate this vulnerability, customers must ensure their Content Update is at version 2120 or higher. This update provides the necessary protection across all supported versions of Cortex XDR. While the Content Update provides the primary fix, the following software releases include complementary architectural enhancements to further harden the environment: * Cortex XDR 9.1.0 (or later) * Cortex XDR 9.0.1 (or later) * Cortex XDR 8.9.1 (or later) * Cortex XDR 8.7.101-CE (or later) Note for 8.3-CE and 7.9-CE: These versions are fully protected by applying Content Update 2120. No additional software upgrade is required for these versions to mitigate this specific vulnerability.

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.