CVE-2026-0232 Cortex XDR Agent: Local Administrator can disable the agent on Windows

Urgency MODERATE

Severity 4 · MEDIUM

Exploit Maturity **UNREPORTED**	Response Effort **MODERATE**	Recovery **USER**	Value Density **DIFFUSE**
Attack Vector **LOCAL**	Attack Complexity **LOW**	Attack Requirements **NONE**	Automatable **YES**
User Interaction **NONE**	Product Confidentiality **NONE**	Product Integrity **NONE**	Product Availability **HIGH**
Privileges Required **HIGH**	Subsequent Confidentiality **NONE**	Subsequent Integrity **NONE**	Subsequent Availability **NONE**

CVE JSON CSAF

Published **2026-04-08**

Updated **2026-04-08**

Discovered **externally**

Description

A problem with a protection mechanism in the Palo Alto Networks Cortex XDR agent on Windows allows a local Windows administrator to disable the agent. This issue may be leveraged by malware to perform malicious activity without detection.

Product Status

Versions	Affected	Unaffected
Cortex XDR Agent 9.1	None on Windows	All on Windows
Cortex XDR Agent 9.0	< 9.0.1 without CU-2120 on Windows	9.0 with CU-2120, >= 9.0.1 on Windows
Cortex XDR Agent 8.9	< 8.9.1 without CU-2120 on Windows	8.9 with CU-2120, >= 8.9.1 on Windows

Cortex XDR Agent 8.7-CE	< 8.7.101-CE without CU-2120 on Windows	8.7-CE with CU-2120, >= 8.7.101-CE on Windows
Cortex XDR Agent 8.3-CE	All without CU-2120 on Windows	All with CU-2120 on Windows
Cortex XDR Agent 7.9-CE	All without CU-2120 on Windows	All with CU-2120 on Windows

Severity: MEDIUM, Suggested Urgency: MODERATE

CVSS-BT: 4.0 / CVSS-B: 6.7
(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/AU:Y/R:U/V:D/RE:M/U:Amber)

Exploitation Status

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

Weakness Type and Impact

CWE-15: External Control of System or Configuration Setting

CAPEC-578 Disable Security Software

Solution

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 and Mitigations

No known workarounds exist for this issue.

Acknowledgments

Palo Alto Networks thanks WhatThe0xDoin for discovering and reporting this issue.

CPEs

cpe:2.3:a:palo_alto_networks:cortex_xdr_agent:9.0.0:*:*:*:*:Windows:*:*

cpe:2.3:a:palo_alto_networks:cortex_xdr_agent:8.9.0:*:*:*:*:Windows:*:*

cpe:2.3:a:palo_alto_networks:cortex_xdr_agent:8.7-CE:*:*:*:*:Windows:*:*

CPE Applicability

- cpe:2.3:a:palo_alto_networks:cortex_xdr_agent:*:*:*:*:*:Windows:*:* **is vulnerable** from (including)9.0.0 **and** up to (excluding)9.0.1
- **OR**cpe:2.3:a:palo_alto_networks:cortex_xdr_agent:*:*:*:*:*:Windows:*:* **is vulnerable** from (including)8.9.0 **and** up to (excluding)8.9.1
- **OR**cpe:2.3:a:palo_alto_networks:cortex_xdr_agent:*:*:*:*:*:Windows:*:* **is vulnerable** from (including)8.7.101 **and** up to (excluding)8.7.101-ce

Timeline

2026-04-08 Initial publication.