CVE-2025-0112: Palo Alto Networks Cortex XDR Agent Allows Local Windows User to Disable the Agent

Vairav Advisory Report

Date: 2025-02-20

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

EXECUTIVE SUMMARY

A vulnerability identified as CVE-2025-0112 has been discovered in the Palo Alto Networks Cortex XDR agent on Windows platforms. This flaw allows local users with non-administrative privileges to disable the agent, potentially enabling malware to deactivate the security agent and execute malicious activities undetected. The vulnerability has been assigned a CVSS score of 6.8 (Medium) severity.

VULNERABILITY DETAILS

CVE-2025-0112

- **Description:** The Cortex XDR agent on Windows contains a flaw in its detection mechanism, permitting users without administrative rights to disable the agent. This vulnerability arises from improper handling of exceptional conditions, which can be exploited by local users or malware to deactivate the agent, leaving the system unprotected against further malicious actions.
- **Impact:** Exploitation of this vulnerability could lead to the deactivation of the Cortex XDR agent, rendering the system vulnerable to unauthorized activities, including data breaches, malware infections, and other malicious operations without detection or prevention.
- **CVSS Score:** 6.8 (Medium)

AFFECTED VERSIONS

The following versions of the Cortex XDR agent on Windows are affected:

- **Cortex XDR Agent 8.5**
  - Versions earlier than 8.5.1
- **Cortex XDR Agent 8.4**
  - All versions (Note: This version reached End-of-Life on February 5, 2025; no further updates or security fixes are planned.)
- **Cortex XDR Agent 8.3-CE**
  - Versions earlier than 8.3.101-CE

EXPLOIT DETAILS

In environments where the Cortex XDR agent is deployed on Windows systems, local users with non-administrative privileges can exploit this vulnerability to disable the agent. This

action compromises the system's security posture, as the deactivated agent can no longer monitor or prevent malicious activities. Malware can also leverage this flaw to disable the agent, facilitating undetected malicious operations.

RECOMMENDED ACTIONS

Patch & Upgrade:

To mitigate this vulnerability, it is recommended to upgrade to the latest versions of the Cortex XDR agent:

- **Cortex XDR Agent 8.5**
  - Upgrade to version 8.5.1 or later
- **Cortex XDR Agent 8.3-CE**
  - Upgrade to version 8.3.101-CE or later

For **Cortex XDR Agent 8.4**, which has reached its End-of-Life, it is strongly recommended to upgrade to a supported version to receive security updates and patches.

ADDITIONAL SECURITY MEASURES

- **Restrict User Privileges**: Ensure that users have the minimum necessary privileges to perform their tasks. Limiting user permissions can reduce the risk of exploitation.
- **Monitor Agent Status**: Implement monitoring to detect and alert if the Cortex XDR agent becomes disabled or inactive, allowing for prompt response to potential exploitation attempts.
- **Regular Security Audits**: Conduct periodic security assessments to identify and remediate vulnerabilities within the environment proactively.

REFERENCES

- https://app.opencve.io/cve/CVE-2025-0112
- https://security.paloaltonetworks.com/CVE-2025-0112

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com