CVE-2024-35177:

IMPROPER ACCESS CONTROL IN WAZUH-AGENT

Vairav Advisory Report

Date: 2025-02-04

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 CVE-2024-35177 has been identified in wazuh-agent. This vulnerability allows an attacker to trigger local escalation of privilege due to improper Access Control List of the non-default installation directory. This could lead to system compromise, security breaches and service disruption.

VULNERABILITY DETAILS

CVE-2024-35177

- **Description:** The root cause is an improper ACL applied on the installation folder when a non-default installation path is specified (e.g.: C:\wazuh). As many DLLs are loaded from the installation folder, by creating a malicious DLL that exports the functions of a legit one, it is possible to escalate privileges from a low-privileged user and obtain code execution under the context of NT AUTHORITY\SYSTEM.
- **Impact:** If exploited, this vulnerability could cause massive impact to a business by causing system compromise, security breaches, data exfiltration and financial and reputational damage.
- **CVSS Score:** 7.8 (High)

AFFECTED VERSIONS

wazuh-agent versions before:

- 4.9.0

EXPLOIT DETAILS

This vulnerability needs two pre-existing conditions to be exploited:

1. The application must be installed in a non-default directory that is writable by default for non-privileged users.
2. The Wazuh service must be restarted or the machine must be rebooted.

If these conditions are met, a low-privileged user can create a DLL that is loaded from the application installation directory that executes some command but that is not found by the application. The DLL is then copied inside the Wazuh agent installation directory and the service is restarted either manually or the machine is rebooted leading to a local privilege escalation that could allow a malicious actor to escalate privileges to the context of those which the wazuh-agent is running under (NT AUTHORITY\SYSTEM)

RECOMMENDED ACTIONS

Patch & Upgrade:

Upgrade to the latest wazuh-agent version:

- 4.9.0

ADDITIONAL SECURITY MEASURES

- Check for unauthorized changes in Wazuh Directories.
- Ensure proper ACLs on Wazuh Installation Directories.
- Block unauthorized DLL injection.
- Monitor service binary and DLL integrity.

REFERENCES

- https://app.opencve.io/cve/CVE-2024-35177
- https://github.com/wazuh/wazuh/security/advisories/GHSA-pmr2-2r83-h3cv

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: mail@vairavtech.com

Website: https://vairavtech.com