NVD DB Update

CVE-2024-35177 - Score: 7.8

Components:

Description:

Wazuh is a free and open source platform used for threat prevention, detection, and response. It is capable of protecting workloads across on-premises, virtualized, containerized, and cloud-based environments. The wazuh-agent for Windows is vulnerable to a Local Privilege Escalation vulnerability due to improper ACL of the non-default installation directory. A local malicious user could potentially exploit this vulnerability by placing one of the many DLL that are loaded and not present on the system in the installation folder of the agent OR by replacing the service executable binary itself with a malicious one. The root cause is an improper ACL applied on the installation folder when a non-default installation path is specified (e.g,: C:\wazuh). Many DLLs are loaded from the installation folder and by creating a malicious DLLs that exports the functions of a legit one (and that is not found on the system where the agent is installed, such as rsync.dll) it is possible to escalate privileges from a low-privileged user and obtain code execution under the context of NT AUTHORITY\SYSTEM. This issue has been addressed in version 4.9.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability.

Main problems:

284 no CWE Description available

https://cybersword.tech
ph1sher
www.linkedin.com/in/cybersword-tech
@davidwowa