NVD DB Update

CVE-2025-24016 - Score: 9.9

Components:

Description:

Wazuh is a free and open source platform used for threat prevention, detection, and response. Starting in version 4.4.0 and prior to version 4.9.1, an unsafe deserialization vulnerability allows for remote code execution on Wazuh servers. DistributedAPI parameters are a serialized as JSON and deserialized using `as\_wazuh\_object` (in `framework/wazuh/core/cluster/common.py`). If an attacker manages to inject an unsanitized dictionary in DAPI request/response, they can forge an unhandled exception (`\_\_unhandled\_exc\_\_`) to evaluate arbitrary python code. The vulnerability can be triggered by anybody with API access (compromised dashboard or Wazuh servers in the cluster) or, in certain configurations, even by a compromised agent. Version 4.9.1 contains a fix.

Main problems:

502 "Deserialization of Untrusted Data"