漏洞檢測

Wazuh 使用漏洞檢測模組來識別在端點上運行的應用程序和操作系統中的漏洞。

這個使用案例展示了 Wazuh 如何檢測被監視端點中未修補的通用漏洞和公開漏洞（CVE）。

有關此功能的更多信息，請參閱文檔中的漏洞檢測部分。

基礎架構

端點

描述

Ubuntu 22.04

這個漏洞檢測模組掃描此 Linux 端點，尋找操作系統和已安裝應用程序中的漏洞。

Windows 11

這個漏洞檢測模組掃描此 Windows 端點，尋找操作系統和已安裝應用程序中的漏洞。

配置

在 Wazuh 伺服器上執行以下步驟，以啟用 Wazuh 漏洞檢測模組。

在 Wazuh 伺服器的/var/ossec/etc/ossec.conf 文件中啟用漏洞檢測模組：

```
<ossec_config>
  <vulnerability-detector>
    <enabled>yes</enabled>
    <interval>5m</interval>
    <min_full_scan_interval>6h</min_full_scan_interval>
    <run_on_start>yes</run_on_start>

    <!-- Ubuntu OS vulnerabilities -->
    <provider name="canonical">
    <enabled>yes</enabled>
    <os>trusty</os>
    <os>xenial</os>
    <os>bionic</os>
    <os>focal</os>
    <os>jammy</os>
    <update_interval>1h</update_interval>
    </provider>

    <!-- Debian OS vulnerabilities -->
    <provider name="debian">
    <enabled>yes</enabled>
    <os>buster</os>
    <os>bullseye</os>
    <update_interval>1h</update_interval>
    </provider>
```

```
    <!-- RedHat OS vulnerabilities -->
    <provider name="redhat">
    <enabled>yes</enabled>
    <os>5</os>
    <os>6</os>
    <os>7</os>
    <os>8</os>
    <os allow="CentOS Linux-8">8</os>
    <os>9</os>
    <update_interval>1h</update_interval>
    </provider>

    <!-- Windows OS vulnerabilities -->
    <provider name="msu">
    <enabled>yes</enabled>
    <update_interval>1h</update_interval>
    </provider>

    <!-- Aggregate vulnerabilities -->
    <provider name="nvd">
    <enabled>yes</enabled>
    <update_from_year>2019</update_from_year>
    <update_interval>1h</update_interval>
    </provider>
  </vulnerability-detector>
</ossec_config>
```

重新啟動 Wazuh 管理器以應用配置更改：

```
sudo systemctl restart wazuh-manager
```

測試配置

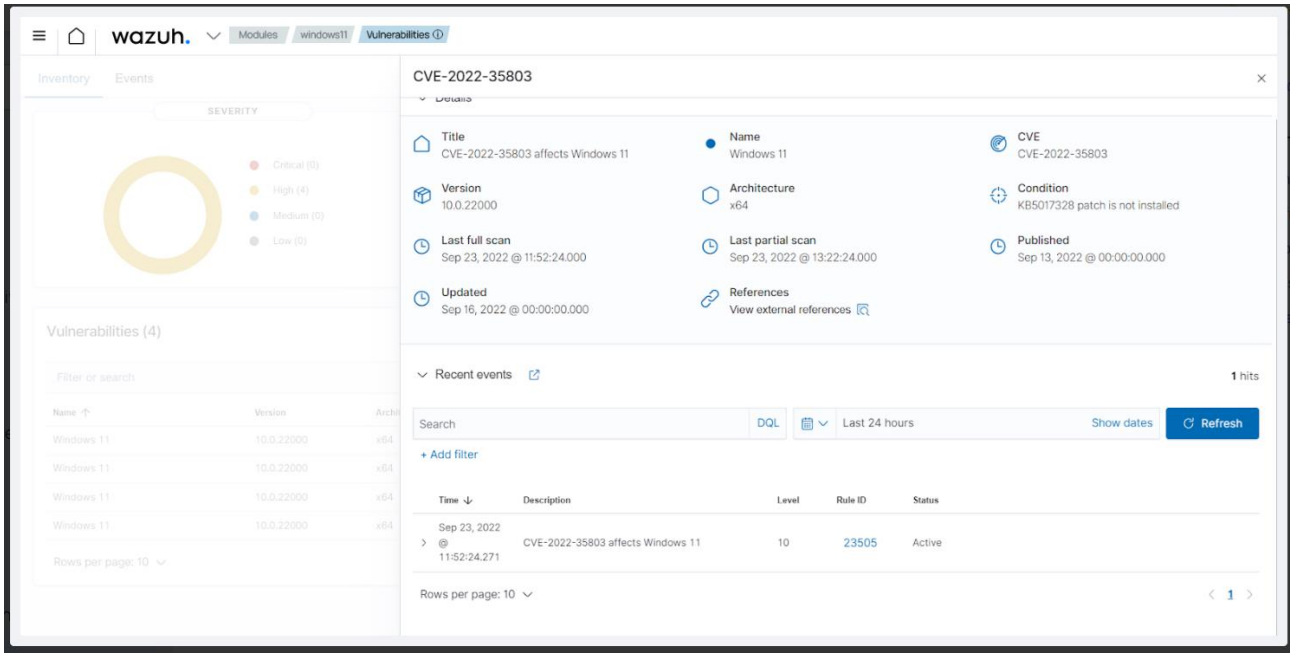
您不需要執行任何操作。Wazuh 伺服器會在/var/ossec/queue/vulnerabilities/cve.db 中創建一個 CVE 數據庫。它會定期對每個被監視端點上的應用程序和操作系統進行漏洞檢測掃描。

注意：根據用戶的網路，下載漏洞數據庫可能需要一些時間。同時，掃描被監視端點上的易受攻擊套件也需要更多時間。

可視化警報資料

您可以在 Wazuh 儀表板中視覺化警報資料。要做到這一點，請前往漏洞檢測模組，選擇一個代理並點擊任何漏洞。

Windows



Ubuntu