Vulnerabilities

Agent	Package	Version	Description	Severity	CVE ID
host01	wheel	0.37.0	A denial-of-service vulnerability exists in PyPA Wheel 0.37.1 and earlier, triggered via attacker-controlled input to the CLI.	High	CVE-2022-40898
host01	setuptools	58.0.4	Remote code execution is possible in `package_index` of `setuptools` up to 69.1.1 via malicious URLs; fixed in 70.0.	High	CVE-2024-6345
host01	setuptools	58.0.4	Remote code execution is possible in `package_index` of `setuptools` up to 69.1.1 via malicious URLs; fixed in 70.0.	High	CVE-2024-6345
host01	future	0.18.2	A DoS vulnerability in Python Charmers Future allows attackers to exploit a crafted Set-Cookie header.	High	CVE-2022-40899
host01	wheel	0.37.0	A denial-of-service vulnerability exists in PyPA Wheel 0.37.1 and earlier, triggered via attacker-controlled input to the CLI.	High	CVE-2022-40898
host01	future	0.18.2	A DoS vulnerability in Python Charmers Future allows attackers to exploit a crafted Set-Cookie header.	High	CVE-2022-40899

CVE-2022-40898

Package: wheel (Python packaging tool)
Version Affected: ≤ 0.37.1
Severity: High
Impact: Attacker-controlled input to the CLI can trigger Denial of Service.
Applies to: macOS (Intel & Apple Silicon), Linux, Windows — wherever wheel is used.

Step 1: Verify the Vulnerable Version

1.1 Check if wheel is installed and version:

pip3 show wheel

You should see something like:
Name: wheel
Version: 0.37.0

```
tiagopaquete@MAC1 ~ % pip3 show wheel
========================================================================
Name: wheel
Version: 0.45.1
…
========================================================================
```

What This Means

You're running wheel version **0.45.1**, which is **well beyond the vulnerable version range** (≤ 0.37.1).

CVE-2022-40898: Add a Custom Rule

1. Navigate to Wazuh rules directory

cd /var/ossec/etc/rules/

```
root@Ubuntu1:~# cd /var/ossec/etc/rules/
root@Ubuntu1:/var/ossec/etc/rules# ls -l
========================================================================
total 4
-rw-rw---- 1 wazuh wazuh 497 Mar 26 20:15 local_rules.xml
========================================================================

root@Ubuntu1:/var/ossec/etc/rules# cat local_rules.xml
========================================================================
<!-- Local rules -->

<!-- Modify it at your will. -->
<!-- Copyright (C) 2015, Wazuh Inc. -->

<!-- Example -->
<group name="local,syslog,sshd,">

  <!--
  Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1
port 1066 ssh2
  -->
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1.</
description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>

</group>
root@Ubuntu1:/var/ossec/etc/rules#
========================================================================
```

2. Add your custom rule inside the `<group>` block, before the closing `</group>` tag

```
<!-- Ignore CVE-2022-40898 -->
<rule id="100002" level="0">
  <description>Ignore alerts related to CVE-2022-40898 in wheel 0.37.0</description>
  <match>CVE-2022-40898</match>
</rule>
```

root@Ubuntu1:/var/ossec/etc/rules# **sudo nano /var/ossec/etc/rules/local_rules.xml**

```
==============================================================================
  GNU nano 7.2                                                    /var/ossec/etc/
rules/local_rules.xml *
<!-- Local rules -->

<!-- Modify it at your will. -->
<!-- Copyright (C) 2015, Wazuh Inc. -->

<!-- Example -->
<group name="local,syslog,sshd,">

  <!--
  Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066
ssh2
  -->
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1.</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>

    <!-- Ignore CVE-2022-40898 -->
  <rule id="100002" level="0">
    <description>Ignore alerts related to CVE-2022-40898 in wheel 0.37.0</
description>
    <match>CVE-2022-40898</match>
  </rule>

</group>


==============================================================================
```

3. Validate the XML file (optional but recommended)

xmllint --noout /var/ossec/etc/rules/local_rules.xml

```
root@Ubuntu1:/var/ossec/etc/rules# xmllint --noout /var/ossec/etc/rules/
local_rules.xml
root@Ubuntu1:/var/ossec/etc/rules#
```

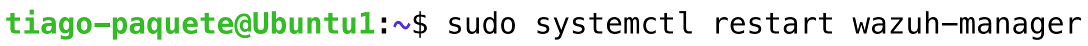
Note:
The command ran without output, which means your local_rules.xml file is valid XML.

Command: xmllint --noout /var/ossec/etc/rules/local_rules.xml

Component	Explanation
xmllint	A command-line XML parser and validator that comes with the libxml2library. It is used to parse XML files, check for syntax errors, and format or query XML data.
--noout	An option that tells xmllint **not to output the content** of the XML file. Instead, it will return only validation results. If the file is valid (well-formed), there will be no output; if there are errors, they will be printed.
/var/ossec/etc/rules/ local_rules.xml	This is the **absolute path** to the XML file being validated. In this case, it points to the local_rules.xml file used by **OSSEC** (an open-source host-based intrusion detection system). This file typically contains custom or local security rules.

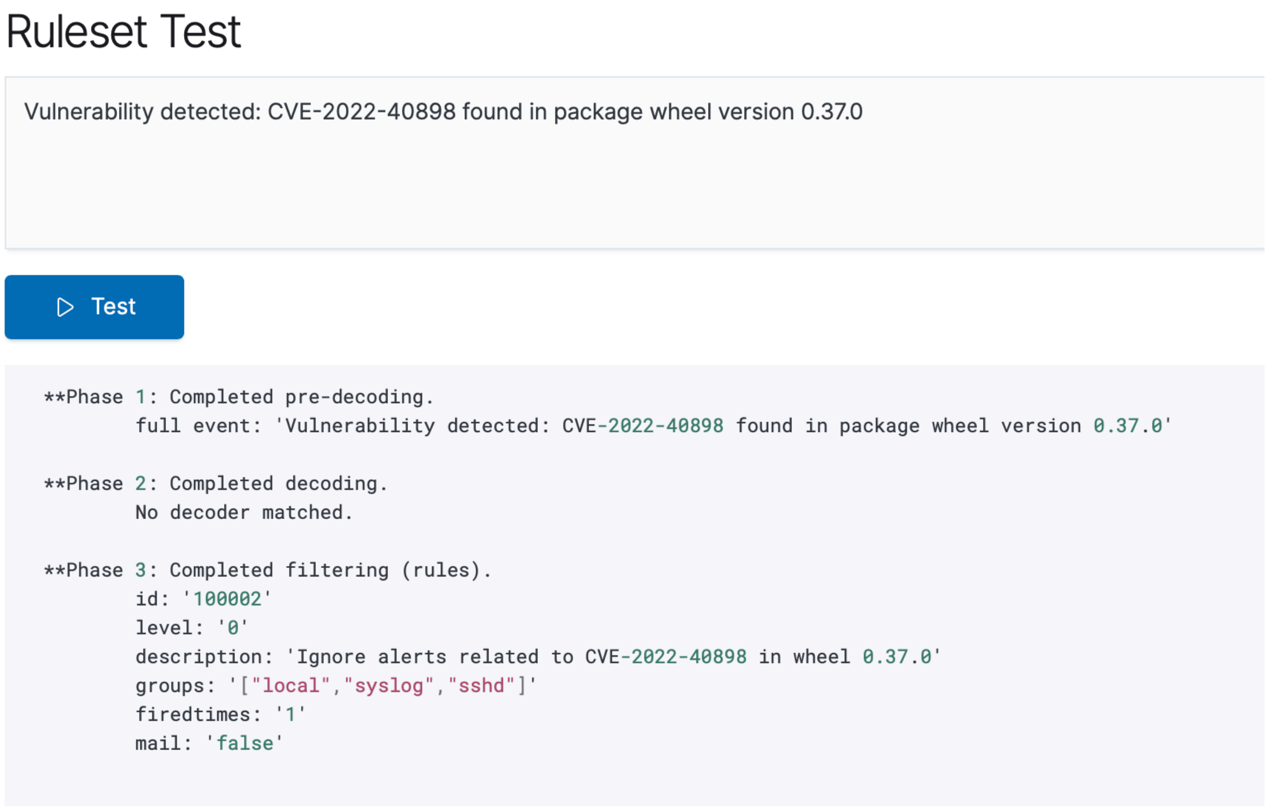
4. Restart the Wazuh manager to apply the rule

sudo systemctl restart wazuh-manager



```
tiago-paquete@Ubuntu1:~$ sudo systemctl restart wazuh-manager
```

5. Ruleset Test



Ruleset Test

Vulnerability detected: CVE-2022-40898 found in package wheel version 0.37.0

```
**Phase 1: Completed pre-decoding.
        full event: 'Vulnerability detected: CVE-2022-40898 found in package wheel version 0.37.0'

**Phase 2: Completed decoding.
        No decoder matched.

**Phase 3: Completed filtering (rules).
        id: '100002'
        level: '0'
        description: 'Ignore alerts related to CVE-2022-40898 in wheel 0.37.0'
        groups: '["local","syslog","sshd"]'
        firedtimes: '1'
        mail: 'false'
```