ossec-hids / etc / rules / clam_av_rules.xml

Julien DUBOIS Updated PCRE2 rules: match_pcre2 replaced by pcre2 d7e933e · 5 years ago

69 lines (57 loc) · 1.83 KB

Code Blame Raw

```
1
2     <group name="clamd,freshclam,">
3
4       <rule id="52500" level="0" noalert="1">
5         <decoded_as>clamd</decoded_as>
6         <description>Grouping of the clamd rules.</description>
7       </rule>
8
9       <rule id="52501" level="0" noalert="1">
10        <decoded_as>freshclam</decoded_as>
11        <description>ClamAV database update</description>
12      </rule>
13
14      <rule id="52502" level="8">
15        <if_sid>52500</if_sid>
16        <pcre2>FOUND</pcre2>
17        <description>Virus detected</description>
18        <group>virus</group>
19      </rule>
20
21      <rule id="52503" level="10">
22        <if_sid>52500</if_sid>
23        <pcre2>^ERROR: </pcre2>
24        <description>Clamd error</description>
25        <group>virus</group>
26      </rule>
```

```
27
28        <rule id="52504" level="7">
29          <if_sid>52500</if_sid>
30          <pcre2>^WARNING: </pcre2>
31          <description>Clamd warning</description>
32          <group>virus</group>
33        </rule>
34
35        <rule id="52505" level="3">
36          <if_sid>52500</if_sid>
37          <pcre2>clamd daemon</pcre2>
38          <description>Clamd restarted</description>
39          <group>virus</group>
40        </rule>
41
42        <rule id="52506" level="3">
43          <if_sid>52500</if_sid>
44          <pcre2>Database modification detected</pcre2>
45          <description>Clamd database updated</description>
46          <group>virus</group>
47        </rule>
48
49        <rule id="52507" level="3">
50          <if_sid>52501</if_sid>
51          <pcre2>ClamAV update process started </pcre2>
52          <description>ClamAV database update</description>
53          <group>virus</group>
54        </rule>
55
56        <rule id="52508" level="3">
57          <if_sid>52501</if_sid>
58          <pcre2>Database updated </pcre2>
59          <description>ClamAV database updated</description>
60          <group>virus</group>
61        </rule>
62
63        <rule id="52509" level="0">
64          <if_sid>52501</if_sid>
65          <pcre2>Incremental update failed|Error while reading database from|Update failed\.</pcre2>
66          <description>Could not download the incremental virus definition updates.</description>
67        </rule>
68
69      </group> <!-- clamd, freshclam -->
```