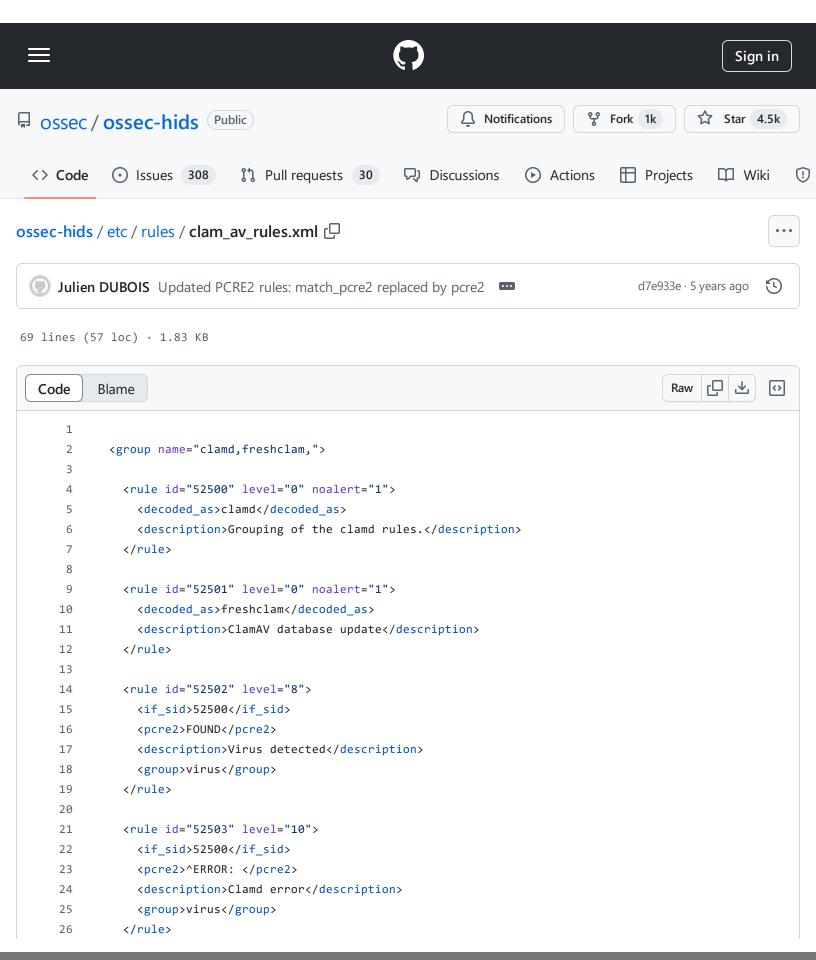
ossec-hids/etc/rules/clam_av_rules.xml at 1ecffb1b884607cb12e619f9ab3c04f530801083 · ossec/ossec-hids · GitHub - 31/10/2024 14:48 https://github.com/ossec/ossec-

hids/blob/1ecffb1b884607cb12e619f9ab3c04f530801083/etc/rules/clam_av_rules.xml



hids/blob/1ecffb1b884607cb12e619f9ab3c04f530801083/etc/rules/clam_av_rules.xml

```
27
28
         <rule id="52504" level="7">
29
           <if sid>52500</if sid>
           <pcre2>^WARNING: </pcre2>
30
           <description>Clamd warning</description>
31
32
           <group>virus
         </rule>
33
34
         <rule id="52505" level="3">
35
36
           <if_sid>52500</if_sid>
37
           <pcre2>clamd daemon</pre2>
           <description>Clamd restarted</description>
38
39
           <group>virus
         </rule>
40
41
         <rule id="52506" level="3">
42
43
           <if sid>52500</if sid>
44
           <pcre2>Database modification detected</pcre2>
           <description>Clamd database updated</description>
45
           <group>virus
46
47
         </rule>
48
49
         <rule id="52507" level="3">
50
           <if sid>52501</if sid>
51
           <pcre2>ClamAV update process started </pcre2>
           <description>ClamAV database update</description>
52
           <group>virus
53
54
         </rule>
55
         <rule id="52508" level="3">
56
57
           <if_sid>52501</if_sid>
58
           <pcre2>Database updated </pre2>
           <description>ClamAV database updated</description>
59
           <group>virus
60
         </rule>
61
62
         <rule id="52509" level="0">
63
           <if_sid>52501</if_sid>
64
           <pcre2>Incremental update failed|Error while reading database from|Update failed\.</pcre2>
65
           <description>Could not download the incremental virus definition updates.</description>
66
         </rule>
67
68
69
       </group> <!-- clamd, freshclam -->
```