

Product Solutions Resources Open Source Enterprise Pricing

Search

Sign in

Sign up

ossec / ossec-hids Public

Notifications Fork 1k Star 4.5k

Code Issues 308 Pull requests 30 Discussions Actions Projects Wiki Security Insights

Files

1ecffb1

Go to file

active-response

contrib

debian\_files

doc

etc

rules

log-entries

translated

apache\_rules.xml

apparmor\_rules.xml

arpwatch\_rules.xml

asterisk\_rules.xml

attack\_rules.xml

cimserver\_rules.xml

cisco-ios\_rules.xml

clam\_av\_rules.xml

courier\_rules.xml

dnsmasq\_rules.xml

dovecot\_rules.xml

dropbear\_rules.xml

exim\_rules.xml

firewall\_rules.xml

firewalld\_rules.xml

ftpd\_rules.xml

hordeimp\_rules.xml

ids\_rules.xml

imapd\_rules.xml

kesl\_rules.xml

last\_rootlogin\_rules.xml

lighttpd\_rules.xml

linux\_usbdetect\_rules.xml

local\_rules.xml

mailscanner\_rules.xml

mcafee\_av\_rules.xml

mhn\_cowrie\_rules.xml

mhn\_dionaea\_rules.xml

ossec-hids / etc / rules / clam\_av\_rules.xml

Julien DUBOIS Updated PCRE2 rules: match\_pcre2 replaced by p... d7e933e · 5 years ago History

Code Blame

69 lines (57 loc) · 1.83 KB

Raw Copy Download Compare

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

<group name="clamd,freshclam,">

<rule id="52500" level="0" noalert="1">

<decoded\_as>clamd</decoded\_as>

<description>Grouping of the clamd rules.</description>

</rule>

<rule id="52501" level="0" noalert="1">

<decoded\_as>freshclam</decoded\_as>

<description>ClamAV database update</description>

</rule>

<rule id="52502" level="8">

<if\_sid>52500</if\_sid>

<pcre2>FOUND</pcre2>

<description>Virus detected</description>

<group>virus</group>

</rule>

<rule id="52503" level="10">

<if\_sid>52500</if\_sid>

<pcre2>^ERROR: </pcre2>

<description>Clamd error</description>

<group>virus</group>

</rule>

<rule id="52504" level="7">

<if\_sid>52500</if\_sid>

<pcre2>^WARNING: </pcre2>

<description>Clamd warning</description>

<group>virus</group>

</rule>

<rule id="52505" level="3">

<if\_sid>52500</if\_sid>

<pcre2>clamd daemon</pcre2>

<description>Clamd restarted</description>

<group>virus</group>

</rule>

<rule id="52506" level="3">

<if\_sid>52500</if\_sid>

<pcre2>Database modification detected</pcre2>

<description>Clamd database updated</description>

<group>virus</group>

</rule>

<rule id="52507" level="3">

<if\_sid>52501</if\_sid>

<pcre2>ClamAV update process started </pcre2>

<description>ClamAV database update</description>







<group>virus</group>

</rule>

<rule id="52508" level="3">

<if\_sid>52501</if\_sid>

Page 1 of 2

-  ms-exchange\_rules.xml
-  ms-se\_rules.xml
-  ms1016\_usbdetect\_rules.xml
-  ms\_dhcp\_rules.xml
-  ms\_firewall\_rules.xml
-  ms ftpd rules.xml

```
57         <!-- <!-- clamd, freshclam -->
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\.<
66         <description>Could not download the incremental virus definition updates.</descript
67     </rule>
68
69 </group> <!-- clamd, freshclam -->
```