

ossec / ossec-hids

Public

Notifications

Fork 1k

Star 4.5k

<> Code

Issues 308

Pull requests 30

Discussions

Actions

Projects

Wiki

Security

Insights

Files

master

Go to file

> .github

> 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

ossec-hids / etc / rules / syslog_rules.xml

Julien DUBOIS

Updated PCRE2 rules: match_pcre2 replaced by p...

d7e933e · 5 years ago

History

Code

Blame

725 lines (584 loc) · 21.4 KB

Raw

1

<!-- @(#) \$Id: syslog_rules.xml,v 1.22 2010/11/25 17:06:17 ddp Exp \$

2

- Official Generic Syslog rules for OSSEC.

3

-

4

- Copyright (C) 2009 Trend Micro Inc.

5

- All rights reserved.

6

-

7

- This program is a free software; you can redistribute it

8

- and/or modify it under the terms of the GNU General Public

9

- License (version 2) as published by the FSF - Free Software

10

- Foundation.

11

-

12

- License details: http://www.ossec.net/en/licensing.html

13

-->

14

15

16

<!-- Default variables for the SYSLOG rules. -->

17

18

<!-- Bad words matching. Any log containing these messages

19

- will be triggered.

20

-->

21

<var name="BAD_WORDS">core_dumped|failure|error|attack| bad |illegal |denied|refused|un

22

23

24

<!-- Syslog errors. -->

25

<group name="syslog,errors,">

26

<rule id="1001" level="2">

27

<pcre2>^Couldn't open /etc/securetty</pcre2>

28

<description>File missing. Root access unrestricted.</description>

29

</rule>

30

31

<rule id="1002" level="2">

32

<pcre2>\${BAD_WORDS}</pcre2>

33

<options>alert_by_email</options>

34

<description>Unknown problem somewhere in the system.</description>

35

</rule>

36

37

<rule id="1003" level="13" maxsize="1025">

38

<description>Non standard syslog message (size too large).</description>

39

</rule>

40

41

<rule id="1004" level="5">

42

<pcre2>^exiting on signal</pcre2>

43

<description>Syslogd exiting (logging stopped).</description>

44

</rule>

45

46

<rule id="1005" level="5">

47

<program_name_pcre2>syslogd</program_name_pcre2>

48

<pcre2>^restart</pcre2>

49

<description>Syslogd restarted.</description>

50

</rule>

51

52

<rule id="1006" level="5">

53

<pcre2>^syslogd \S+ restart</pcre2>

54

<description>Syslogd restarted.</description>

55







</rule>

56

57

<rule id="1007" level="7">

Page 1 of 11

-  mhn_dionaea_rules.xml
-  ms-exchange_rules.xml
-  ms-se_rules.xml
-  ms1016_usbdetect_rules.xml
-  ms_dhcp_rules.xml
-  ms firewall rules.xml

```
57 <rule id="1007" level="1">
58   <pcre2>file system full|No space left on device</pcre2>
59   <description>File system full.</description>
60   <group>low_diskspace,</group>
61 </rule>
62
63 <rule id="1008" level="5">
64   <pcre2>killed by SIGTERM</pcre2>
65   <description>Process exiting (killed).</description>
66   <group>service_availability,</group>
67 </rule>
68
69 <rule id="1009" level="0">
70   <if_sid>1002</if_sid>
71   <pcre2>terminated without error|can't verify hostname: getaddrinfo|</pcre2>
72   <pcre2>PPM exceeds tolerance</pcre2>
73   <description>Ignoring known false positives on rule 1002.</description>
74 </rule>
75
76 <rule id="1010" level="5">
77   <pcre2>segfault at </pcre2>
78   <description>Process segfaulted.</description>
79   <group>service_availability,</group>
80 </rule>
81 </group> <!-- SYSLOG,ERRORS -->
82
83
84
85 <!-- NFS messages -->
86 <group name="syslog,nfs,">
87   <!-- XXX All These NFS rules need to be fixed. -->
88   <rule id="2100" level="0" noalert="1">
89     <program_name_pcre2>^automount|^mount</program_name_pcre2>
90     <description>NFS rules grouped.</description>
91   </rule>
92
93   <rule id="2101" level="4">
94     <if_sid>2100</if_sid>
95     <pcre2>nfs: mount failure</pcre2>
96     <description>Unable to mount the NFS share.</description>
97   </rule>
98
99   <rule id="2102" level="4">
100     <if_sid>2100</if_sid>
101     <pcre2>reason given by server: Permission denied</pcre2>
102     <description>Unable to mount the NFS directory.</description>
103   </rule>
104
105   <rule id="2103" level="4">
106     <pcre2>^rpc\.mountd: refused mount request from</pcre2>
107     <description>Unable to mount the NFS directory.</description>
108   </rule>
109
110   <rule id="2104" level="2">
111     <if_sid>2100</if_sid>
112     <pcre2>lookup for \S+ failed</pcre2>
113     <description>Automount informative message</description>
114   </rule>
115 </group> <!-- SYSLOG,NFS -->
116
117
118
```


652 <group>config_changed,</group>
653 <description>Yum package deleted.</description>

```
654     </rule>
655
656     <!-- SCSI CONTROLLER -->
657     <rule id="2935" level="0" noalert="1">
658       <if_sid>5100</if_sid>
659       <id_pcre2>mptscsih</id_pcre2>
660       <description>Grouping for the mptscrih rules.</description>
661     </rule>
662
663     <rule id="2936" level="0" noalert="1">
664       <if_sid>5100</if_sid>
665       <id_pcre2>mptbase</id_pcre2>
666       <description>Grouping for the mptbase rules.</description>
667     </rule>
668
669     <rule id="2937" level="12">
670       <if_sid>2935</if_sid>
671       <status_pcre2>FAILED</status_pcre2>
672       <description>Possible Disk failure. SCSI controller error.</description>
673     </rule>
674
675     <rule id="2938" level="12">
676       <if_sid>2936</if_sid>
677       <action>failed</action>
678       <description>SCSI RAID ARRAY ERROR, drive failed.</description>
679     </rule>
680
681     <rule id="2939" level="12">
682       <if_sid>2936</if_sid>
683       <action>degraded</action>
684       <description>SCSI RAID is now in a degraded status.</description>
685     </rule>
686
687     <rule id="2940" level="0">
688       <program_name_pcre2>^NetworkManager</program_name_pcre2>
689       <description>NetworkManager grouping.</description>
690     </rule>
691
692     <rule id="2941" level="3">
693       <if_sid>2940</if_sid>
694       <pcre2> No chain/target/match by that name\.$</pcre2>
695       <description>Incorrect chain/target/match.</description>
696     </rule>
697
698     <rule id="2942" level="0">
699       <if_sid>1002</if_sid>
700       <pcre2>g_slice_set_config: assertion `sys_page_size == 0' failed</pcre2>
701       <description>Uninteresting gnome error.</description>
702     </rule>
703
704     <rule id="2943" level="0">
705       <pcre2>^nouveau </pcre2>
706       <description>nouveau driver grouping</description>
707     </rule>
708
709     <rule id="2944" level="1">
710       <if_sid>2943</if_sid>
711       <pcre2> DATA_ERROR BEGIN_END_ACTIVE$| DATA_ERROR$</pcre2>
712       <description>Uninteresting nouveau error.</description>
713     </rule>
714
715     <rule id="2945" level="4">
716       <program_name_pcre2>^rsyslogd</program_name_pcre2>
717       <pcre2>^imuxsock begins to drop messages </pcre2>
718       <info>https://isc.sans.edu/diary/Are+you+losing+system+logging+information+%28and+d
719       <description>rsyslog may be dropping messages due to rate-limiting.</description>
720     </rule>
721
722   </group>
723
724
725   <!-- EOF -->
```

