


 **Julien DUBOIS** Updated PCRE2 rules: match\_pcre2 replaced by pcre2  d7e933e · 5 years ago 


122 lines (98 loc) · 4.21 KB


Code

Blame

Raw







```
1      <!-- @(#) $Id: ./etc/rules/attack_rules.xml, 2011/09/08 dcid Exp $
2
3      - Official "attack" correlation rules for OSSEC.
4      -
5      - Copyright (C) 2009 Trend Micro Inc.
6      - All rights reserved.
7      -
8      - This program is a free software; you can redistribute it
9      - and/or modify it under the terms of the GNU General Public
10     - License (version 2) as published by the FSF - Free Software
11     - Foundation.
12     -
13     - License details: http://www.ossec.net/en/licensing.html
14     -->
15
16
17     <!-- System users. They should never log in to the system -->
18     <var name="SYS_USERS">^apache$|^mysql$|^www$|^nobody$|^nogroup$|^portmap$|^named$|^rpc$|^mail$|^ftp
19
20
21     <!-- Attack signatures -->
22     <group name="syslog,attacks,">
23         <rule id="40101" level="12">
24             <if_group>authentication_success</if_group>
25             <user_pcre2>$SYS_USERS</user_pcre2>
26             <description>System user successfully logged to the system.</description>
```

```
27     <group>invalid_login,</group>
28 </rule>
29
30 <rule id="40102" level="14">
31   <pcre2>^rpc\.statd\[d+\]: gethostbyname error for [^A-Za-z0-9@_-]+</pcre2>
32   <description>Buffer overflow attack on rpc.statd</description>
33   <group>exploit_attempt,</group>
34 </rule>
35
36 <rule id="40103" level="14">
37   <pcre2>ftpd\[d+\]: \S+ FTP LOGIN FROM .+ 0bin0sh</pcre2>
38   <description>Buffer overflow on WU-FTPD versions prior to 2.6</description>
39   <group>exploit_attempt,</group>
40 </rule>
41
42 <rule id="40104" level="13">
43   <pcre2>\?{21}</pcre2>
44   <description>Possible buffer overflow attempt.</description>
45   <group>exploit_attempt,</group>
46 </rule>
47
48 <rule id="40105" level="12">
49   <pcre2>changed by \\(\\(null\\)</pcre2>
50   <description>"Null" user changed some information.</description>
51   <group>exploit_attempt,</group>
52 </rule>
53
54 <rule id="40106" level="12">
55   <pcre2>@{25}</pcre2>
56   <description>Buffer overflow attempt (probably on yppasswd).</description>
57   <group>exploit_attempt,</group>
58 </rule>
59
60 <rule id="40107" level="14">
61   <pcre2>cachefs: Segmentation Fault - core dumped</pcre2>
62   <description>Heap overflow in the Solaris cachefs service.</description>
63   <info type='cve'>2002-0033</info>
64   <group>exploit_attempt,</group>
65 </rule>
66
67 <rule id="40109" level="12">
68   <pcre2>attempt to execute code on stack by</pcre2>
69   <description>Stack overflow attempt or program exiting </description>
70   <description>with SEGV (Solaris).</description>
71   <info type="link">http://snap.nlc.dcccd.edu/reference/sysadmin/julian/ch18/389-392.html</info>
72   <group>exploit_attempt,</group>
```

```
73     </rule>
74
75     <rule id="40111" level="10" frequency="10" timeframe="160">
76       <if_matched_group>authentication_failed</if_matched_group>
77       <description>Multiple authentication failures.</description>
78       <group>authentication_failures,</group>
79     </rule>
80
81     <rule id="40112" level="12" timeframe="240">
82       <if_group>authentication_success</if_group>
83       <if_matched_group>authentication_failures</if_matched_group>
84       <same_source_ip />
85       <description>Multiple authentication failures followed </description>
86       <description>by a success.</description>
87     </rule>
88
89     <rule id="40113" level="12" frequency="6" timeframe="360">
90       <if_matched_group>virus</if_matched_group>
91       <description>Multiple viruses detected - Possible outbreak.</description>
92       <group>virus,</group>
93     </rule>
94
95 </group> <!-- SYSLOG, ATTACKS, -->
96
97
98
99 <!-- Privilege escalation messages -->
100 <group name="syslog,elevation_of_privilege,">
101   <rule id="40501" level="15" timeframe="300" frequency="2">
102     <if_group>adduser</if_group>
103     <if_matched_group>attacks</if_matched_group>
104     <description>Attacks followed by the addition </description>
105     <description>of an user.</description>
106   </rule>
107 </group> <!-- SYSLOG, ELEVATION_OF_PRIVILEGE, -->
108
109
110
111 <!-- Scan signatures -->
112 <group name="syslog,recon,">
113   <rule id="40601" level="10" frequency="10" timeframe="90" ignore="90">
114     <if_matched_group>connection_attempt</if_matched_group>
115     <description>Network scan from same source ip.</description>
116     <same_source_ip />
117     <info type="link">http://project.honeynet.org/papers/enemy2/</info>
118   </rule>
```

```
118         </rule>
119     </group> <!-- SYSLOG, SCANS -->
120
121
122     <!-- EOF -->
```