Sign in

ossec / ossec-hids Public

Notifications Fork 1k Star 4.5k

Code Issues 308 Pull requests 30 Discussions Actions Projects Wiki

ossec-hids / etc / rules / syslog_rules.xml

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

725 lines (584 loc) · 21.4 KB

Code Blame Raw

```xml
<!-- @(#) $Id: syslog_rules.xml,v 1.22 2010/11/25 17:06:17 ddp Exp $
  -  Official Generic Syslog rules for OSSEC.
  -
  -  Copyright (C) 2009 Trend Micro Inc.
  -  All rights reserved.
  -
  -  This program is a free software; you can redistribute it
  -  and/or modify it under the terms of the GNU General Public
  -  License (version 2) as published by the FSF - Free Software
  -  Foundation.
  -
  -  License details: http://www.ossec.net/en/licensing.html
  -->


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

<!-- Bad words matching. Any log containing these messages
  -  will be triggered.
  -->
<var name="BAD_WORDS">core_dumped|failure|error|attack| bad |illegal |denied|refused|unauthorized|f


<!-- Syslog errors. -->
<group name="syslog,errors,">
  <rule id="1001" level="2">
```

```
    <pcre2>^Couldn't open /etc/securetty</pcre2>
    <description>File missing. Root access unrestricted.</description>
  </rule>

  <rule id="1002" level="2">
    <pcre2>$BAD_WORDS</pcre2>
    <options>alert_by_email</options>
    <description>Unknown problem somewhere in the system.</description>
  </rule>

  <rule id="1003" level="13" maxsize="1025">
    <description>Non standard syslog message (size too large).</description>
  </rule>

  <rule id="1004" level="5">
    <pcre2>^exiting on signal</pcre2>
    <description>Syslogd exiting (logging stopped).</description>
  </rule>

  <rule id="1005" level="5">
    <program_name_pcre2>syslogd</program_name_pcre2>
    <pcre2>^restart</pcre2>
    <description>Syslogd restarted.</description>
  </rule>

  <rule id="1006" level="5">
    <pcre2>^syslogd \S+ restart</pcre2>
    <description>Syslogd restarted.</description>
  </rule>

  <rule id="1007" level="7">
    <pcre2>file system full|No space left on device</pcre2>
    <description>File system full.</description>
    <group>low_diskspace,</group>
  </rule>

  <rule id="1008" level="5">
    <pcre2>killed by SIGTERM</pcre2>
    <description>Process exiting (killed).</description>
    <group>service_availability,</group>
  </rule>

  <rule id="1009" level="0">
    <if_sid>1002</if_sid>
    <pcre2>terminated without error|can't verify hostname: getaddrinfo|</pcre2>
    <pcre2>PPM exceeds tolerance</pcre2>
    <description>Ignoring known false positives on rule 1002..</description>
  </rule>

  <rule id="1010" level="5">
    <pcre2>segfault at </pcre2>
    <description>Process segfaulted.</description>
    <group>service_availability,</group>
  </rule>
</group> <!-- SYSLOG,ERRORS -->



<!-- NFS messages -->
<group name="syslog,nfs,">
  <!-- XXX All These NFS rules need to be fixed. -->
  <rule id="2100" level="0" noalert="1">
    <program_name_pcre2>^automount|^mount</program_name_pcre2>
    <description>NFS rules grouped.</description>
  </rule>

  <rule id="2101" level="4">
    <if_sid>2100</if_sid>
    <pcre2>nfs: mount failure</pcre2>
    <description>Unable to mount the NFS share.</description>
  </rule>

  <rule id="2102" level="4">
    <if_sid>2100</if_sid>
    <pcre2>reason given by server: Permission denied</pcre2>
    <description>Unable to mount the NFS directory.</description>
  </rule>

  <rule id="2103" level="4">
    <pcre2>^rpc\.mountd: refused mount request from</pcre2>
    <description>Unable to mount the NFS directory.</description>
  </rule>

  <rule id="2104" level="2">
    <if_sid>2100</if_sid>
    <pcre2>lookup for \S+ failed</pcre2>
    <description>Automount informative message</description>
  </rule>
</group> <!-- SYSLOG,NFS -->
```

```
    <group>config_changed,</group>
    <description>Yum package deleted.</description>
  </rule>

  <!-- SCSI CONTROLLER -->
  <rule id="2935" level="0" noalert="1">
    <if_sid>5100</if_sid>
    <id_pcre2>mptscsih</id_pcre2>
    <description>Grouping for the mptscrih rules.</description>
  </rule>

  <rule id="2936" level="0" noalert="1">
    <if_sid>5100</if_sid>
    <id_pcre2>mptbase</id_pcre2>
    <description>Grouping for the mptbase rules.</description>
  </rule>

  <rule id="2937" level="12">
    <if_sid>2935</if_sid>
    <status_pcre2>FAILED</status_pcre2>
    <description>Possible Disk failure. SCSI controller error.</description>
  </rule>

  <rule id="2938" level="12">
    <if_sid>2936</if_sid>
    <action>failed</action>
    <description>SCSI RAID ARRAY ERROR, drive failed.</description>
  </rule>

  <rule id="2939" level="12">
    <if_sid>2936</if_sid>
    <action>degraded</action>
    <description>SCSI RAID is now in a degraded status.</description>
  </rule>

  <rule id="2940" level="0">
    <program_name_pcre2>^NetworkManager</program_name_pcre2>
    <description>NetworkManager grouping.</description>
  </rule>

  <rule id="2941" level="3">
    <if_sid>2940</if_sid>
    <pcre2> No chain/target/match by that name\.$</pcre2>
    <description>Incorrect chain/target/match.</description>
  </rule>

  <rule id="2942" level="0">
    <if_sid>1002</if_sid>
    <pcre2>g_slice_set_config: assertion `sys_page_size == 0' failed</pcre2>
    <description>Uninteresting gnome error.</description>
  </rule>

  <rule id="2943" level="0">
    <pcre2>^nouveau </pcre2>
    <description>nouveau driver grouping</description>
  </rule>

  <rule id="2944" level="1">
    <if_sid>2943</if_sid>
    <pcre2> DATA_ERROR BEGIN_END_ACTIVE$| DATA_ERROR$</pcre2>
    <description>Uninteresting nouveau error.</description>
  </rule>

  <rule id="2945" level="4">
    <program_name_pcre2>^rsyslogd</program_name_pcre2>
    <pcre2>^imuxsock begins to drop messages </pcre2>
    <info>https://isc.sans.edu/diary/Are+you+losing+system+logging+information+%28and+don%27t+know+
    <description>rsyslog may be dropping messages due to rate-limiting.</description>
  </rule>

</group>


<!-- EOF -->
```