Cacti Vulnerability in perfSONAR-PS Toolkit Details.

There has been a vulnerability in the Cacti component of the perfSONAR-PS Toolkit identified which can allow "defacing" of the text fields on the Cacti settings web page or possible SQL injection attack into the Cacti database. It exists in versions of perfSONAR-PS prior to the following RPM versions:

```
 perl-perfSONAR_PS-Toolkit-SystemEnvironment-3.3.2-16.pSPS.noarch
 perl-perfSONAR_PS-Toolkit-3.3.2-16.pSPS.noarch
 perl-perfSONAR_PS-Toolkit-LiveCD-3.3.2-16.pSPS.noarch
```

Problem Remediation

The RPMS (and the corresponding updated ISOs) listed in the previous section address the issue. The patch created (that will be pulled down via yum) disables 'guest' (e.g. anonymous) access to cacti on the toolkit. The ink on the main page is still there, but will now require someone with a password/username to get in. This prevents unauthenticated access to the Cacti settings page, removing the threat of "defacing" or SQL injection.

For our recommended *netinstall* (installation onto local disk) sites should 'yum update'. This is as simple as:

```
yum  -y  update
reboot
```

For sites running from CD or USB, please download, produced updated media and reboot your system using the updated media.

Disabling Cacti

Since Cacti is NOT part of either the OSG or WLCG perfSONAR-PS use-cases, sites can choose to disable it entirely via:

1. Edit /etc/httpd/conf.d/apache-toolkit_web_gui.conf
2. Add the following stanza:

   ```
   <Directory "/opt/perfsonar_ps/toolkit/web/root/admin/cacti">
     Deny from all
   </Directory>
   ```

3. Restart apache:

   ```
    sudo /etc/init.d/httpd restart
   ```

Then any access attempt will result in a 403 return.

Verification of Fix

Sites can verify they have the updated RPMS via *rpm -qa | grep PS-Toolkit*. Check for the 3.3.2-16 versions mentioned at the top of the page.

Alternately you can try to access the Cacti settings page to verify it prompts for authentication. The form of the URL is

```
http://<perfSONAR_FQDN>/toolkit/gui/cacti/graph_settings.php
```

For example, if your toolkit instance is psum01.aglt2.org you should verify http://psum01.aglt2.org/toolkit/gui/cacti/graph_settings.php prompts you for authentication.

References

See EGI SVG EGI-SVG-2014-7162 or refer to perfSONAR-PS FAQ at http://psps.perfsonar.net/toolkit/FAQs.html#Q77.

-- ShawnMcKee - 26 Jun 2014

This topic: LCG > CactiperfSONAR
Topic revision: r1 - 2014-06-26 - ShawnMcKee