

Cross-scripting Vulnerability in JOWPING (perf of perfSONAR-PS Toolkit) Details.

OWPING, a java client for the OWAMP measurement tool, has been found to be vulnerable to a form of cross site scripting involving manipulation of HTTP headers. The perfSONAR-PS Toolkit developer's analysis has found that chance of exploit is remote (e.g. cannot be done with simple URL manipulation or Javascript), but warrants action by the toolkit deployers. The recommendation is that sites with concerns remove JOWPING from their servers using the following command:

```
> sudo rm -rf /opt/perfsonar_ps/toolkit/web/root/gui/jowping/
```

This will result in a broken link on the left sidebar, but removes the software and the risk. A recent update to the 3.3.x series of the pS Performance Toolkit removed JOWPING completely, and this tool was already earmarked to not be present on the upcoming 3.4 release due to lack of a maintainer.

The development team would like to thank John Parker from NOAA, who found this vulnerability through routine use of the skipfish tool (<http://code.google.com/p/skipfish>). Feel free to relay any questions or concerns you have to the developers.

Thanks;

The perfSONAR Development Team

The versions below (or more recent) have removed JOWPING and are not vulnerable:

```
perl-perfSONAR_PS-Toolkit-SystemEnvironment-3.3.2-17.pSPS.noarch  
perl-perfSONAR_PS-Toolkit-3.3.2-17.pSPS.noarch  
perl-perfSONAR_PS-Toolkit-LiveCD-3.3.2-17.pSPS.noarch
```

Problem Remediation

The RPMS listed in the previous section address the issue.

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, this is not yet a new image out with the fix (as of 18-July-2014). Instead you can remove jowping via:

```
sudo rm -rf /opt/perfsonar_ps/toolkit/web/root/gui/jowping/
```

References

See perfSONAR mailing lists for announcement of the issue and remediation:

<http://comments.gmane.org/gmane.comp.networking.perfsonar.user/748>

-- ShawnMcKee - 18 Jul 2014

This topic: LCG > JowPingperfSONAR

Topic revision: r1 - 2014-07-18 - ShawnMcKee



Copyright &© 2008-2019 by the contributing authors. All material on this collaboration platform is the property of the contributing authors.

Ideas, requests, problems regarding TWiki? Send feedback