Vulnerability for perfSONAR Deployments

Multiple vulnerabilities allowing unauthenticated remote users to run arbitrary code with the privileges of the user that runs Bash scripts was found in Bourne Again Shell (Bash). This has been called the 'shellshock vulnerability (CVE-2014-6271) and has been widely publicized.

Starting on September 25th, the perfSONAR developers sent announcements to their mailing lists highlighting the bash vulnerability. All perfSONAR users and administrators are encouraged to join these lists:

- https://lists.internet2.edu/sympa/subscribe/perfsonar-announce
- https://lists.internet2.edu/sympa/subscribe/perfsonar-user

Advisories have been sent by the EGI CSIRT concerning this:
https://wiki.egi.eu/wiki/EGI_CSIRT:Alerts/Shellshock-2014-09-29

It was discovered that attackers have taken advantage of this vulnerability to compromise a significant number of perfSONAR instances in the high energy physics community. Security teams are actively investigating with the identified victims.

Attackers continue to aggressively use the Bash vulnerability to attack perfSONAR instances.

The security teams, as well as WLCG Operations, **highly recommend that all sites terminate their perfSONAR instances** as a precautionary measure, until the attacks are contained. Easiest option is to just power-off your perfSONAR nodes.

(Unless you have patched the Bash packages on your perfSONAR by Friday 26 Sep **and** have sufficient expertise to ensure your host has not been compromised.)

The following FAQ lists the details of the CVEs found:
https://access.redhat.com/articles/1200223#faq_six_CVE_assignments

NOTE: We understand that there could be further patches (after September 26th). Currently CentOS has the following patch announcements:

- http://lists.centos.org/pipermail/centos-announce/2014-September/020585.html
- http://lists.centos.org/pipermail/centos-announce/2014-September/020593.html

Please do not hesitate to contact your local or infrastructure security team in case of questions:

- EGI CSIRT: abuse@egiNOSPAMPLEASE.eu
- OSG Security Team: security@opensciencegridNOSPAMPLEASE.org
- perfSONAR Developer Team: perfsonar-developer@internet2NOSPAMPLEASE.edu

Further details are covered below.

Indicators of a Compromised System

The log files are one of the best sources of information. Scanning through the host's `/var/log/httpd/access_log*` files for requests using the bash environment variable parsing '() { :;};' is one thing to check for.

Since a number of sites were incorporated into BotNets, system admins may want to reference this paper describing BotNets and their detection:

http://www.giac.org/paper/gsec/4095/snort-detect-rogue-irc-bot-programs/106586

In general, the remote compromises into perfSONAR toolkit instances would operate with the privileges of the user operating the web server. This user would typically be `apache` but check your `./etc/httpd/conf/httpd.conf` file to confirm.

Since compromises could come from many different attackers of varying expertise it may be safest to rebuild any host which

1. Wasn't patched before September 26th
2. Has not been reviewed by experts to verify it is not compromised.

Remediation

We are recommending that perfSONAR hosts be rebuilt as the best and easiest form of remediation. While there are scripts provided by the perfSONAR project that will allow users to preserve their data, we are not sure that they might inadvertently copy components of a compromised system as well. Therefore a 'clean' rebuild is recommended. Current users of the LiveCD should strongly consider transitioning to the use of NetInstall instead.

We note that the release of perfSONAR 3.4 is imminent and expected sometime during the week of October 6th. Sites should wait for the 3.4 release to be out before rebuilding. Installation details will be available at https://code.google.com/p/perfsonar-ps/wiki/pSPerformanceToolkit34#Installation The WLCG perfSONAR deployment details are documented at https://twiki.cern.ch/twiki/bin/view/LCG/PerfsonarDeployment

-- The WLCG Network and Transfer Metrics WG - 29 Sep 2014

This topic: LCG > ShellShockperfSONAR
Topic revision: r6 - 2014-10-01 - ShawnMcKee