Server Automation Alert:
Shell Shock Linux Batch Bug Vulnerability

(December 16, 2014)

ACTION: Update SA core server OS with Vendor Patch Release. Update Server Automation with the documented instruction.
The information in this alert should be acted upon right away.

Change Table for this Document

Date	Change
September 29, 2014	Initial Release
Oct 24, 2014	Added reference to Rollup Hot Fix under Immediate Mitigation section
Dec 16, 2014	Added umask 0022 command to the Immediate Mitigation section.

Issue that Requires Attention

GNU Bash exposed two vulnerabilities: CVE-2014-6271 and CVE-2014-7169.

The currently deployed versions of bash (prior to 4.3.025) in Linux platform contain a vulnerability which allows function definitions as values in environment variables.

If these environment variables are exported in the script, they execute as soon as the script runs. This may lead to arbitrary code execution if a malicious user is able to set the input for an exported environment variable. In this case code will be executed with the privileges of the user running bash.
Vulnerability Origin:

- Apache using mod_cgi – web services could be subverted remotely
- Services using restricted SSH functionality such as Git or Subversion could be subverted remotely
- DHCP clients could be tricked into executing code at system level and allow an attacker on the network to subvert an entire datacentre

How to verify if a Linux OS is affected?

To test if your version of Bash is vulnerable to this issue, run the following command:
$ env x='() { :;}; echo vulnerable' bash -c "echo this is a test"
If the output of the above command looks as follows:
vulnerable
this is a test
Then it proves you are using a vulnerable version of Bash. Thus, if you run the above command with the patched version of Bash, you should get an output similar to:
bash: warning: x: ignoring function definition attempt
bash: error importing function definition for `x' this is a test

Note: See also the following HPSW Security Bulletin:

Impact on SA

General

SA restrict external entities to access SA network endpoint through SA gateway ingress map and egress filter. This protects SA cores and managed servers from accessing by arbitrary remote endpoint. In addition, SA core and managed servers also communicate over SSL with two-way authentication. Generally, the managed servers are not allowed to communicate with each other. This further limits the allowable remote access point pairs in the deployment. To our current best knowledge, the known vulnerabilities are 1. Between managed servers and core component servers 2. Among core component servers. All impacted OSs on both core components and managed servers should be patched.

SA Core

SA Core is the central command center for SA system. It has access to all managed servers. It is crucial that the customer prioritizes its OS and SA specific patching over individual managed server's OS patching.

One of the HP SA component, Opsware Global Shell (ogsh) uses GNU Bash as the internal shell and the version used (3.2) is one of the affected versions.

Even though the Bash used within ogsh is internal to HP SA and does not expose it for immediate known attack vectors, as a precaution we are providing manual steps to update the Bash shell on an existing HP SA install.

Since OGSH runs on the core (infrastructure and slice hosts of HPSA), from the ogsh point of view our scope is limited to core platforms where HPSA is supported. i.e. Redhat, SUSE, OEL and Solaris (for HPSA 9.0x) and centos (for SAVA).

The solution we are suggesting here is for the existing customers to use a fixed bash.

Immediate Mitigation

Fix the bash used by ogsh

In general for all flavors of Unix (HPSA core platforms) the following steps are performed

- Update the system bash to a version where the vulnerability is fixed.
- Replace the bash at /var/opt/opsware/ogfs/mnt/root/bin with the fixed version of bash.

```
# cp /bin/bash /opt/opsware/ogfsutils/bin/bash
# # make sure umask is set to 0022
# umask 0022
# /opt/opsware/ogfs/tools/rewink
# /opt/opsware/ogfs/tools/reload
```

- Launch ogsh and test if the vulnerability is fixed.

Fix with updated Rollup Hot Fix

Alternatively customers can also obtain the latest Hot Fix (Rollup Hot Fix) from SA Support. Below are current version with the fix:

Product	Crypt Patch ID	Availability
SA 9.15	ROLLUP_9.15.011_54731	Now
SA 9.16	ROLLUP_9.16.005_54730	Now
SA 10.01	SAENT_ROLLUP_10.01.005_53656	Now
SA 10.02	SAENT_ROLLUP_10.02.002_54732	Now
SA 10.10	SAENT_ROLLUP_10.10.002_54737	Now

Long Term Solution

We also compile bash 3.2 source and ship it with HPSA. This is delivered to /opt/opsware/ogfsutils/bin/bash. Now we are asking customers to copy /bin/bash to /opt/opsware/ogfsutils/bin/bash. In the upcoming release we will be fixing bash3.2 source and deliver a fixed version of bash.

SA Managed Server

SA managed server needs to be OS patched.

SA DHCP Server

SA may use external DHCP servers for OS Provisioning. These DHCP servers need to be OS patched.