Server Automation Alert:
GHOST: glibc Vulnerability (CVE-2015-0235)

Document Release Date: February 13, 2015
Affected SA Releases (a.k.a. Enterprise or Ultimate editions of SA): 9.1x, 10.0x, 10.1x, 10.2x
Affected SAVA Releases (a.k.a. Standard or Premium editions of SA): 10.0x

ACTION: Use the instructions in this alert to update Server Automation cores.
This information should be acted upon immediately.

Change Table for this Document

Date	Change
Feb 13, 2015	Initial Release
March 4, 2015	Added information regarding SA 10.0x Standard Edition (a.k.a. SA Virtual Appliance (SAVA))

Issue that Requires Attention

glibc Vulnerability: CVE-2015-0235

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0235

Note: This link provides further information about this issue and lists the glibc versions affected.

HP has investigated the CVE-2015-0235 glibc security vulnerability (GHOST) in relation to Server Automation (SA). This document provides required actions you must perform to mitigate this vulnerability.

Note: For SA 10.0x Standard Edition (aka SAVA), please install the **Patch update for SAVA 10.02**. Download patch and instructions are provided on the HP Software Support Self-Solve portal at:

https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/LID/SRVA_00189 (HP Passport credentials required)

Impact on SA

SA components use glibc, which is installed on the operating system that hosts your cores, slices, and satellites. Operating systems, ogfs binaries, .iso images, and PXE images that use glibc are vulnerable to the GHOST security threat. As a result of the HP investigation into this threat, HP recommends that you perform the mitigating actions described in the next section.

Immediate Mitigation Actions

Perform the actions in this section to address the glibc security vulnerability.

1. Update your glibc version on the operating system that hosts your cores, slices, and satellites. Use one of the following links to access glibc-updating procedures for your specific platform:

   RedHat Enterprise Linux: **https://access.redhat.com/articles/1332213**

   SUSE Linux Enterprise: **http://support.novell.com/security/cve/CVE-2015-0235.html**

   Oracle Enterprise Linux: **http://linux.oracle.com/cve/CVE-2015-0235.html**

   Note: Oracle Solaris 10 SPARC (still supported as a platform in Hubble 9.1x versions) is not vulnerable as it does not use glibc.

2. Perform *one* of the following actions:

   a. (Preferred) Complete a system reboot to clear out the memory cache. Clearing the cache makes sure that glibc-running processes will use the updated glibc version.

   b. Use the `service opsware-sas restart` command to restart all SA components on every core, slice, and satellite.

3. Use the commands below to rebuild the ogfs binaries with the rewink/reload mechanism on the systems that host your cores and slices (you do not need to rebuild the ogfs binaries on systems that host

satellites).

Note: Set `umask` to 0022.

```
# umask 0022
# /opt/opsware/ogfs/tools/rewink
# /opt/opsware/ogfs/tools/reload
```

4. Update the following vulnerable OS provisioning .iso images as soon as HP releases the updates:

```
Library->By Folder->OS Provisioning: HPSA_linux_boot_cd.iso
Library->By Folder->OS Provisioning: HPSA_linux_boot_cd_IA64.iso
Library->By Folder->OS Provisioning: HPSA_linux_boot_cd_x86-
64.iso
```

   These .iso images are used during OS provisioning staging of a Red Hat Enterprise Linux Server in a non-DHCP environment.

   HP expects to release updated .iso images as soon as possible after Red Hat releases their images with vulnerability fixes (Red Hat versions 7.1, 6.7, and 5.12). For more information on Red Hat releases, see: **https://access.redhat.com/articles/3078**.

5. Upgrade outdated vulnerable PXE boot images as soon as HP releases the updates.

   These images are required to boot from the network during Linux OS provisioning.
   HP expects to release updated boot images as soon as possible after Red Hat releases their updated installation images. When the updated boot images are released, use the following Knowledge Base article to install the images: **KM1112458** .