Server Automation

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

Note: This information should be acted upon immediately.

Software version: 9.1x, 10.0x, 10.1x, 10.2x (Enterprise or Ultimate editions of SA); 10.0x SAVA (Standard or Premium editions)

Document release date: February 2015

Software release date: 2014

Contents

Impact on SA 2

Immediate mitigation actions 2

Send documentation feedback 3

Legal notices 3

- Warranty 3
- Restricted rights legend 3
- Copyright notice 3
- Trademark notices 3
- Documentation updates 3
- Support 3

Impact on SA

Issue that requires attention: glibc Vulnerability: CVE-2015-0235

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

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

HPE 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), install the *Patch update for SAVA 10.02*. Download patch and instructions are provided on the HPE Software Support Self-Solve portal at:

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

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 HPE investigation into this threat, HPE 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 HPE 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.

   HPE 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 HPE releases the updates.

   These images are required to boot from the network during Linux OS provisioning.
   HPE 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 .

Send documentation feedback

If you have comments about this document, you can send them to hpe_sa_docs@hpe.com.

Legal notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted rights legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright notice

Trademark notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

RED HAT READY™ Logo and RED HAT CERTIFIED PARTNER™ Logo are trademarks of Red Hat, Inc.

The OpenStack word mark and the Square O Design, together or apart, are trademarks or registered trademarks of OpenStack Foundation in the United States and other countries, and are used with the OpenStack Foundation's permission.

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to the following URL and sign-in or register: https://softwaresupport.hpe.com/

Select Manuals from the Dashboard menu to view all available documentation. Use the search and filter functions to find documentation, whitepapers, and other information sources.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your Hewlett Packard Enterprise sales representative for details.

Support

Visit the Hewlett Packard Enterprise Software Support Online web site at https://softwaresupport.hpe.com/