HP Server Automation Alert: CVE-2015-0240 Samba Update

Document Release Date: March 20, 2015
Affected Releases: 9.1x up to 9.17, 10.0x up to 10.03, 10.1x up to 10.11, 10.2x up to 10.21

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

Issue that Requires Attention 2
Impact on Server Automation 2
Mitigation Actions 2

Change Table for this Document

Date	Change
Mar 19, 2015	Initial Release

Issue that Requires Attention

CVE-2015-0240 Samba: Unexpected code execution in smbd vulnerability
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0240

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

HP has investigated the CVE-2015-0240 Samba security vulnerability in relation to Server Automation. This document provides required actions that must be performed to mitigate this vulnerability.

Impact on Server Automation

Server Automation distributes its own Samba as part of the OPSWsamba rpm package. Samba is used as the Media Server used during provisioning of Microsoft Windows servers. Versions 9.1x up to 9.17, 10.0x up to 10.03, 10.1x up to 10.11, 10.2x up to 10.21 contain Samba versions that are vulnerable to CVE-2015-0240. The installed Samba version can be determined by executing the command `/opt/opsware/samba/sbin/smbd --version`.

Mitigation Actions

You can avoid being impacted by the CVE-2015-0240 Samba vulnerability in the following ways:

1. If you don't do provisioning for Microsoft Windows Servers you can disable the Samba daemon from running.
2. If you do provisioning for Microsoft Windows Servers, it is necessary to upgrade Samba by installing the patch as described below.

1. Disable Samba from running

To disable Samba from running perform the following actions while connected via SSH on a Core:

```
# stop the Samba daemon from running
[root@sa-core ~]# service opsware-sas stop smb
>>> Stopping smb ...
Shutting down SMB services:                                [  OK  ]
Shutting down NMB services:                                [  OK  ]
Successfully performed "stop" operation on Opsware SAS components.

# to ensure that the Samba daemon will not start at boot
# edit the /opt/opsware/oi_util/startup/components.config file
# and comment out the 2 lines referring to smb:
[root@sa-core ~]# grep --after-context=2 'smb'
/opt/opsware/oi_util/startup/components.config
#smb        $STARTUP/smb            $VERIFY_PRE \
#           $VERIFY_POST            $VERIFY_FUNCTIONALITY2. Install the Samba patch
```

2. Install the patch for Samba

The patch upgrades the Samba daemon installed on a Server Automation Core to version 3.6.25.

The following table contains links where the patch can be downloaded for each Server Automation version:

Server Automation version	Patch download link
Server Automation 9.1x	https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/LID/SRVA_00190
Server Automation 10.0x	https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/LID/SRVA_00191
Server Automation 10.1x	https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/LID/SRVA_00192
Server Automation 10.2x	https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/LID/SRVA_00193

To install it, download the zip archive corresponding to your Server Automation version from softwaresupport.hp.com, copy the archive to the Core(s)/Satellites which have the OPSWSamba rpm package installed, extract it and execute the `patch.sh` command (replace SRVA_00190.zip with the filename that applies to your Server Automation version):

```
[root@sa-core ~]# unzip SRVA_00190.zip
[root@sa-core ~]# tar xf SRVA_00190.tar.gz
[root@sa-core ~]# cd saent_samba_3.6.25_update_59281
[root@sa-core saent_samba_3.6.25_update_59281]# ./patch.sh install
Install patch: CVE-2015-0240
Processed 1 patches

# check the version of the smbd and nmbd binaries
[root@sa-core saent_samba_3.6.25_update_59281]# /opt/opsware/samba/sbin/smbd –version
Version 3.6.25
[root@sa-core saent_samba_3.6.25_update_59281]# /opt/opsware/samba/sbin/nmbd –version
Version 3.6.25
```

The patch can be uninstalled with the following procedure:

```
# from the directory where the .tar.gz archive with the patch was extracted:
[root@sa-core saent_samba_3.6.25_update_59281]# ./patch.sh remove
Removing patch: CVE-2015-0240
Processed 1 patches

# to confirm that the removal was successful
# check the version of the smbd and nmbd binaries
[root@sa1020 saent_samba_3.6.25_update_59281]# /opt/opsware/samba/sbin/smbd –version
Version 3.6.22
[root@sa1020 saent_samba_3.6.25_update_59281]# /opt/opsware/samba/sbin/nmbd –version
Version 3.6.22
```

Notes:

- During installation, if the OPSWsamba rpm package is not installed or the patch is already installed, the `patch.sh install` command will respond with `No patches needed`.
- During removal, if the OPSWsamba rpm package is not installed or the patch is already removed or not installed, the `patch.sh remove` command will respond with `Nothing to uninstall`.