Hardware Management Console Readme

For use with Version 8 Release 8.5.0

Date: 19 August 2016

Contents

The information in this Readme contains the fix list and other package information about the Hardware Management Console.

PTF MH01651

This package includes fixes for HMC Version 8 Release 8.5.0. You can reference this package by APAR MB04035 and PTF MH01651. This image must be installed on top of HMC Version 8 Release 8.5.0 Recovery DVD (PTF MH01616) with mandatory PTF MH01617 installed.

Note: This PTF supersedes MH01640 and MH01649.

Package information

Package name	Size	Checksum (sha1sum)	APAR#	PTF#
MH01651.iso	1537341440	7d75d1dd5d0a1f2dd6fa688335ef2013bfa0437c	MB04035	MH01651
Splash Panel information (or lshmc -V output)				
"version= Version: 8 Release: 8.5.0 Service Pack: 0 HMC Build level 20160811.1 MH01617: Required fix for HMC V8R8.5.0 (05-20-2016) MH01651: Fix for HMC V8R8.5.0 (08-11-2016) ","base_version=V8R8.5.0 "				

Known Issues

1. **Special Install Instructions:** Installing this PTF using the Enhanced+ interface may hang. Prior to installing this PTF using the web browser graphical interface perform the following:

1. Log in again selecting the Log In option of "Classic".
2. If already logged in to the HMC using Enhanced GUI, log off the HMC.
3. Install using the normal installation instructions.

Alternatively, install this PTF using the CLI updhmc command.

Command line change

- Enhanced the chhmcencr and lshmcencr commands to support user configuration of the encryption ciphers and Message Authentication Code (MAC) algorithms used by the HMC Secure Shell (SSH) interface.

List of fixes

Security Fixes

- Fixed Apache Tomcat Vulnerability: CVE-2016-3092.
- Fixed multiple NTP vulnerabilities: CVE-2015-7703, CVE-2016-1547, CVE-2016-1548, CVE-2016-1550, and CVE-2016-2518.
- Fixed multiple OpenSSH vulnerabilities: CVE-2015-6563, CVE-2015-6564, CVE-2016-3115, and CVE-2016-1908.
- Fixed IBM Websphere Application Server (WAS) vulnerability: CVE-2016-2923

General fixes

- Updated the expiration date for the vterm applet. The current certificate expires August 25th 2016.
- Fixed an issue where, after successfully applying a concurrent server firmware update, the HMC Change Licensed Internal Code panel could show an incorrect pending deferred firmware level. The problem does not impact the GUI view levels task or lslic command. This issue is only exposed by a rare type of concurrent server firmware update which has never been released in the field but could occur in the future.
- Fixed an issue where HMC backups to a remote server may fail with *rc=26 permission denied* when the remote user has write access to the target. The problem only occurs when a previous backup was done and the remote user does not have the permissions to overwrite an existing RemoteAccessFile.Test file.
- Fixed a problem where HMC to HMC communication intermittently fails resulting in serviceable event B3036620. Other symptoms include failure to negotiate a primary HMC for problem analysis which can result in failure to report a server serviceable event or calling home the same event twice. Repeated occurrences of the B3036620 without a HMC reboot can eventually lead to a hang of the HMC where users are unable to login via the GUI or run commands via ssh.
- Fixed a problem causing the WLP server not to start after the HMC is rebooted, causing the REST API functions to not be available. This impacts the enhanced GUI login, PowerVC, PCM and any other function that utilizes the REST API on the HMC. This

problem only occurs if the user runs the save upgrade data task and subsequently reboots the HMC without actually performing an HMC upgrade. This fix prevents the problem from occuring again and also repairs HMCs previously impacted.
- Fixed a problem where user configured ipv4 static routes were ignored. netstat -rn showed that kernel routing table was never updated to include the static routes.
- Fixed an issue where call home could fail when ISAS mode was enabled. This only impacts HMCs that manage IBM "solutions" where the HMC was modified to call home the server using a different model/type then the server being managed. Impacted "solutions" include HMCs that are part of IBM Elastic Storage Server (ESS) and PurePower.
- Fixed a rare issue where problem numbers for servicable events on HMC model 7042-CR9 may not be unique.
- Fixed a rare issue where call home operations of the problem Extended Error Data (EED) failed due an internal error.
- Fixed an issue where after installing a PTF the security mode could not be changed due to an "Invalid Parameter" error from chhmc command.
- Fixed a validation problem with the virtualFCMappings parameter of the REST API RemoteRestart operation. The problem caused an error to be returned when more than one virtual fibre channel mapping was specified. This issue may impact PowerVC initiated remote restart operations.

Previously released fixes also included in this PTF:

MH01649 07/20/16	• Fixed an issue where problem Call Home fails when the "State or Province" field in the customer information is blank. This impacts all countries outside the US and Canada.
MH01640 06/28/16	• Added functionality to the chhmc command to allow an admin to set a grub password at bootup. • Fixed openSSL vulnerabilities: CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, and CVE-2016-2109 • Fixed security scan vulnerability by enabling TLSv1.2 by default for HMC vterm port (9960) when HMC is in Legacy mode. • Fixed Java vulnerability: CVE-2016-3426 • Fixed Power Hardware Management Console: CVE-2016-0230 • Fixed an issue with installing HMC R8 V8.5.0 onto HMC hardware model 7042-CR9 if the version of SMBIOS is greater than v2.8. The install fails with "*The current system does not have a valid machine type/model. Installation cannot be performed*." • Fixed an issue where the call home from the Manage Dumps panel was uploading incomplete data. • Fixed an issue to prevent call home of SRC E2FF1801 during software

	transmissions.

Installation

Special Install Instructions: Installing this PTF using the Enhanced+ interface may hang. Prior to installing this PTF using the web browser graphical interface perform the following:

1. Log in again selecting the Log In option of "Classic".
2. If already logged in to the HMC using Enhanced GUI, log off the HMC.
3. Install using the normal installation instructions.

Alternatively, Install this PTF using the CLI updhmc command

Installation instructions for HMC Version 8 upgrades and corrective service can be found at these locations:

Upgrading or restoring HMC Version 8

Installation methods for HMC Version 8 fixes

Instructions and images for upgrading via a remote network install can be found here:

HMC V8 network installation images and installation instructions

Additional information

Notes:

1. The Install Corrective Service task now allows you to install corrective service updates from the ISO image files of these updates. You can download these ISO image files for the HMC, and then use the ISO image file to install the corrective service update. You no longer need to burn CD-R or DVD-R media to use the ISO image file to install corrective service.
2. This image requires DVD -R media.
3. To install updates over the network, select the *.iso file on the "Select Service Package" panel of the Install Corrective Service task. The HMC application extracts the files needed to install the corrective service. If you are using USB flash media, copy the *.iso file to the flash media, and then select the file when prompted.
4. The **updhmc** command line command has also been modified to use the *.iso file. To use the command, follow the syntax in this example:

   ```
   updhmc -t s -h <myservername> -f </home/updates/corrrective_service.iso> -u <HMC_username> -i
   ```

In all cases, the HMC application extracts the files needed to install the corrective service.