Hardware Management Console Readme

For use with Version 8 Release 8.2.0

Contents

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

- [PTF MH01486](#)
- [Package information](#)
- [List of fixes](#)
- [Installation](#)
- [Additional information](#)

PTF MH01486

This package includes a fix for HMC Version 8 Release 8.2.0. You can reference this package by APAR MB03871 and PTF MH01486. This image must be installed on top of HMC Version 8 Release 8.2.0 with mandatory PTF MH01454.

Package information					
Package name	**Size**	**Checksum (sha1sum)**		**APAR#**	**PTF#**
MH01486.iso	47760179 2	f2687978d59bc95b266d0652e76045f38fcf85f 2		MB0387 1	MH0148 6
Splash Panel information (or lshmc -V output)					
"version= Version: 8 Release: 8.2.0 Service Pack: 0 HMC Build level 20141203.1 MH01454: Required fix for HMC V8R8.2.0 (11-05-2014) MH01486: Fix for HMC V8R8.2.0 (12-12-2014) ","base_version=V8R8.2.0 "					

List of fixes

Enhancements

- This PTF disables SSLv3 on the HMC user interfaces. After applying this PTF, remote access to the HMC (Browser, ASM, GUI vterm, and pegasus) will require clients that support TLSv1.0 IBM i secure remote 5250 console will require TLSv1.1 or higher. The PTF also disables all ciphers except TLSv1.2 on HMC/FSP connections where the server firmware level supports it.

- Enhanced the chpwrmgmt and lspwrmgmt commands to support a new power saver mode of fixed_max_frequency .

- For HMCs set to security mode nist_sp800_131a, this PTF changes the HMC-Server FSP encryption mode to enforce TLS1.2. This implies that all POWER6 and POWER7 servers must be upgraded to a firmware level that supports TLS1.2 prior to apply of this PTF when using nist_sp800_131a security mode.

Security Fixes

This PTF includes fixes for the following security vulnerabilities:

- CVE-2014-3513, CVE-2014-3567, CVE-2014-3568, CVE-2014-3566, CVE-2014-3567, CVE-2014-3568, CVE-2014-6512, CVE-2014-3566, CVE-2014-6457, CVE-2014-6558

General fixes

- Fixed a problem where the HMC incorrectly reports Serviceable Event E212E112.
- Fixed a problem where the backup critical console task using sFTP fails with error HSCP0198 when the sftp server does not support the df command.
- Provided a new descriptive error message for when a simplified remote restart enabled partition, cross HMC migration attempt fails due to a downlevel target HMC.
- Fixed a problem where heavy use of REST API can cause the HMC to fail or lockup due to too many open file handles.

Installation

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.