# Hardware Management Console Readme

For use with Version 8 Release 8.4.0 Service Pack 1
Updated: 28 June 2016

### Contents

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

# PTF MH01639

This package includes fixes for HMC Version 8 Release 8.4.0 Service Pack 1. You can reference this package by APAR MB04026 and PTF MH01639. This image must be installed on top of HMC Version 8 Release 8.4.0 Service Pack 1 (PTF MH01576) with or without additional fixes.

**Note**: This PTF supersedes PTF MH01626 and MH01632.

<table>
<tr><td colspan="5"><i>Package information</i></td></tr>
<tr><th>Package name</th><th>Size</th><th>Checksum (sha1sum)</th><th>APAR#</th><th>PTF#</th></tr>
<tr><td>MH01639.iso</td><td>1537472512</td><td>a6ebf4848568ef1c81900bbb79055d5d07ecb019</td><td>MB04026</td><td>MH01639</td></tr>
<tr><th colspan="5">Splash Panel information (or lshmc -V output)</th></tr>
<tr><td colspan="5">"version= Version: 8<br> Release: 8.4.0<br> Service Pack: 1<br> HMC Build level 20160615.1<br> MH01639: Fix for HMC V8R8.4.0 SP1 (06-15-2016)<br> ","base_version=V8R8.4.0<br> "</td></tr>
</table>

# 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

2. After installing this PTF, the security mode cannot be changed. The **chhmc -c security -s modify --mode nist_sp800_131a** command will fail with "*Invalid Parameter*".

# Command line changes

This PTF adds a new option to the chhmc command to allow an admin to set a grub password at bootup. To resolve this security vulnerability, users apply the PTF (with mandatory reboot) then set a password.

Syntax:

```
chhmc -c grubpasswd
        -s {enable | disable | modify}
        [--passwd password]
```

- To enable and set the password
  ```
  chhmc -c grubpasswd -s enable --passwd password
  ```

- To disable the grub password
  ```
  chhmc -c grubpasswd -s  disable
  ```

- To modify the grub password
  ```
  chmc -c grubpasswd -s  modify --passwd password
  ```

# List of fixes

### Security Fixes

- 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 an issue where a user was unable to connect to enhanced GUI in NIST mode because of the following cipher in cipher list: TLS_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
- Fixed Power Hardware Management Console: CVE-2016-0230

### General Fixes

- Fixed an issue where backing up the HMC included PCM data even though the user did not select to include PCM data.
- Fixed an issue where the Console Window > Open Terminal Window task may fail with "*javax.net.ssl.SSLProtocolException: handshake alert: unrecognized_name*" in Java console output.
- Fixed an issue where a newly added usb device did not get an entry in the /etc/fstab table impacting lshw calls.
- Fixed an issue where the call home from the Manage Dumps panel was uploading incomplete data.
- Disabled keyboard shortcut feature for all GUI panels.
- Fixed an error seen after restoring a critical console data backup, error after login is "*Not Found. The application or context root for this request has not been found:/rest/ui/static/RedirectCCFWLogon*".
- Fixed a chatlet exception to prevent call home SRC E3550046.

- Added a fix to check for potential X configuration failures and to subsequently reset display configs to defaults in order to avoid "*out of range*" failures.
- Fixed an issue with the TF4 display which extended outside of the viewable pane.
- Fixed an issue with dynamically removing adapters that may result in error "*Error Rendering Task Panel. An unrecoverable error has occurred while rendering a task's graphical output. An attempt has been made to terminate the task. Any operation in progress may have been interrupted prematurely. An entry in the error log has been created so this problem can be reported automatically.*"
- Fixed an issue to prevent call home of SRCs E355104B and E355104D.
- Fixed an issue with chhmc where adding a nameserver failed silently.

**Previously released fixes also included in this PTF:**

| | |
|---|---|
| **MH01632**<br>05/15/16 | • Enhanced logging for serviceable event E212E122 logged against /dev.<br>• Fixed an issue where the Console Window > Open Terminal Window task fails to open a vterm window when launched from the local HMC and the HMC does not have internet access.<br>• Fixed an issue where call home of serviceable events could try to use the legacy (pre-V8R8.3.0) callhome servers if an error is returned contacting the new call home servers.<br>• Fixed an issue where the  Console Window > Open Terminal Window may fail with "*javax.net.ssl.SSLProtocolException: handshake alert: unrecognized_name*" in Java console output. |
| **MH01626**<br>04/25/16 | • Fixed the following OpenSSL security vulnerabilities: CVE-2015-3197, CVE-2016-0702, CVE-2016-0705, CVE-2016-0797<br>• Fixed Tomcat vulnerabilities: CVE 2015-5174,CVE-2015-5345,  CVE-2015-5346, CVE-2015-5351, CVE-2016-0706, CVE-2016-0714, CVE-2016-0763<br>• Fixed vulnerabilities in bind: CVE-2016-1285  and CVE-2016-1286<br>• Fixed security vulnerability with Strongswan; CVE-2015-8023<br>• Fixed the following Httpd security vulnerabilities; CVE-2013-5704 CVE-2015-3183<br>• Fixed libssh2 security vulnerability: CVE-2016-0787<br>• Fixed NTP security vulnerabilities: CVE-2015-5300, CVE-2015-7704, CVE-2015-8138<br>• Fixed a problem where port 12443 may allow ciphers outside the list of current ciphers as defined by lshmcencr/chhmcencr.<br>• Fixed a security issue with HMC restricted shell.<br>• Fixed a performance issue where the Format media panel can take 30 seconds or more to list USB devices.<br>• Fixed a rare issue where Serviceable Events E35A0017 and E35A0016 may be reported due to a deadlock related to HMC data replication services.<br>• Fixed an issue where call home was attempting to establish a connection to the old (pre HMC V8R8.3.0) callhome servers even when not using legacy callhome.  If the legacy callhome addresses were blocked by a firewall, call home may fail.<br>• Fixed  a problem where scheduled HMC backups configured for FTP failed with rc=23 if the remote FTP server did not also support SFTP.<br>• Fixed an error obtaining credentials that resulted in call home SRC E3D4310A. |

# Installation

**Special Install Instructions:** This fix must be installed using the HMC updhmc command or the classic login "update HMC task"; not the enhanced GUI login.

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.