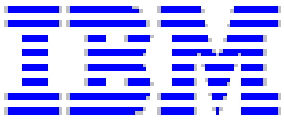

IBM System x™

Firmware Update Best Practices

IMM, UEFI, FPGA, and DSA Preboot

Revision date: February 15, 2012

Table of Contents

1 Introduction

Firmware updates are important to insure your system is reliable and performing to its maximum capacity. The Intel-based server line is an extremely open platform where hardware components, operating systems, and software applications come from a multitude of different vendors and the market is constantly churning out new hardware and software. By the time a system has been fully loaded, there may be code from dozens of sources. While every vendor tests their code to the best of their ability, it is impossible to test every possible configuration of hardware and software that can exist. It is therefore inevitable that sometimes vendors will learn about an incompatibility after the product or the system software update has already been released. Most of these lessons are learned early in a product's system software lifecycle, so fewer and fewer service packs, hot fixes, and firmware updates are required as the product and system software mature.

Updates are used to provide performance and usability enhancements, new features, and bug fixes. Some of these fixes correct problems in the vendor's own code, but many also address compatibility issues between one vendor's elements (application, operating system, hardware) and the elements from other vendors. Updates provide a way for the manufacturer to improve compatibility, features, performance, availability, etc. for their customers.

In some cases, it is extremely important to synchronize updates. Most hardware components come with firmware and a driver. Hardware vendors also provide management software for some hardware components. When a vendor releases a new driver with new firmware and/or management software, the vendor expects the customer to update all of the elements together. Unpredictable results may occur if these elements get out of sync. In most cases, a condition of support will be that the hardware system software and /or management software are at the proper release level.

1.1 Adopt a strategy

Due to the frequency of updates from hardware and software vendors, it is virtually impossible to apply every update that is released, and no one would recommend that this be done. By the same token, it is very dangerous to live by the "if it ain't broke, don't fix it" mantra. Some firmware and device driver fixes are designed to prevent data corruption, data loss or to plug security holes. Other fixes address memory leaks or system halts that relate directly to server downtime. These fixes should clearly be applied in a timely manner when servers are "at risk."

Most bug fixes can be tracked back to a problem that a customer reported. The fix will be important to that customer, but it may or may not be important to other customers. Most vendors provide information to help customers determine if they have systems that are at risk and to quantify the seriousness of the risk.

Updates that address less critical issues may also be important down the road. A large percentage of the calls placed to technical support are resolved when the customer applies an update that was previously posted to the web. Had these updates been applied as part of a regular maintenance cycle, they would have enjoyed more reliable systems and lower support costs.

It is therefore important for you to adopt an update strategy and define an orderly update process. The best strategy and process will vary from customer to customer, but the following questions should be answered:

- How do we know when/if a problem is identified that puts our servers at risk?

- How frequently do we perform routine maintenance?
- How do we manage updates?
- How do we know that updates will not introduce new problems?

1.2 Monitoring for change

Resolving critical issues before they cause downtime is something that can only be done if you have access to the proper information at the proper time, so your change management plan needs to be as flexible as your environment.

Best Practices:

- Subscribe to proactive email notifications from ibm.com for updates for your servers. You can subscribe from the Notifications section of the Support home page (http://www.ibm.com/support/entry/portal/Overview).
- Regularly monitor critical update notifications for your systems and/or set up a task to review them at least every 45 days.

1.3 Frequency of routine maintenance

Since most updates occur early in an element's (application, operating system, hardware) life cycle, it is extremely important to update frequently when using a new element such as hardware or operating systems. Also, organizations that are making frequent hardware/software configuration changes are less likely to encounter problems if their system software is maintained with up-to-date code. Many companies will have multiple environments, and different update cycles may be appropriate for each environment.

IBM posts bundles of firmware and drivers called a UXSP (UpdateXpress System Pack) to ibm.com on a quarterly basis. In between UXSPs, IBM may post firmware and driver updates to support new hardware or fix critical bugs.

Best Practices:

- Install the UXSP for your system unless you need the latest driver or firmware not contained in that package to provide support for new hardware or to fix a specific problem you're encountering. In this case start from the baseline of the UXSP then supplement it with any individual code updates.
- Quarterly updates are recommended for dynamic environments and those using new hardware or operating systems.
- Semiannual updates are recommended for most customer environments.
- Annual updates should be adequate for static environments using mature technology.

1.4 Managing the updates

Whenever possible maintain all system software at the appropriate levels for the particular environment. Have a clearly defined methodology for performing updates.

Best Practices:

- Adopt a controlled, methodical approach.
- Apply to test systems first.
- In production, apply updates starting with low-impact servers and slowly move to business-critical servers.

- Select times for performing updates based on when they will least impact your business.
- Don't update too many systems at a time. Make sure you have the resources required to recover should problems develop.

1.5 Managing the risks

How do you know that updates will not introduce new problems? Risk is inevitable with change, and no one would claim otherwise. The goal of performing regular updates is to manage the change, and thereby manage the risk. When change is managed properly, problems occur less frequently and are usually easier to solve. When change is not managed, you can encounter unexpected or unanticipated outages.

When the best practices outlined above are followed, change can be effectively managed, but there are a few additional tasks that are important to any change management activity:

Best Practices:

- Maintain a log of all configuration and code changes made to your systems
- Log all unusual events and problems
- Keep the logs where other people can access them
- Review logs as part of "problem determination"

1.6 Recommended firmware update methods

There are multiple methods with unique and individual procedures for performing firmware updates. The preferred methods to perform firmware updates are to use the ToolsCenter UpdateXpress System Pack Installer (UXSPI) or Bootable Media Creator (BoMC). These tools are able to:

- Display an inventory of installed firmware and drivers
- Download firmware and drivers from ibm.com
- Download a UXSP from ibm.com
- Update all of the firmware and drivers in your system, including RAID, HDD, NIC, and Fibre Channel devices
- Apply updates in the correct order to completely update a system with the fewest reboots
- Create a bootable CD/DVD/USB key/PXE image to perform firmware updates (BoMC)

Note: Media created by BoMC can only do firmware updates.

See Additional Information for links to UXSPI and BoMC.

1.7 What's new – Integrated Management Module (IMM)

- New levels of manageability. Not only does the IMM provide the base management controller (BMC) function for the system, but it can optionally provide remote presence and control features to manage, monitor, troubleshoot and repair remotely.
- The IMM includes features such as the following:
  - Single firmware image for IMM across the product set.
  - Ability to remotely configure IMM and UEFI settings without the server powered on.

- Ability to update DSA Preboot firmware via the IMM web interface and the ability to update the IMM, UEFI, and FPGA firmware via the IMM and AMM web interfaces.
- Standards based interfaces including IPMI and SNMP (v1 and v3).
- Upward integration with IBM Systems Director.
- An internal LAN over USB interface to allow high speed communication between the operating system and the IMM. This is in addition to the legacy KCS IPMI interface which is common with previous BMC function.

Note: Because the IMM is running a full operating system, it takes time to initialize. Once the IMM's operating system is up and running, the IMM starts the services and interfaces required to monitor the server. The IMM then brings up the rest of the internal services and external interfaces such as the web interface. Because of this, after updating the IMM, you must wait up to 17 minutes (depending on the update method and system configuration) for the IMM to be ready before initiating any further firmware updates. This initialization timeframe may be unexpected to those unfamiliar with the new IMM technology.

1.8 What's new – Unified Extensible Firmware Interface (UEFI)

The Unified Extensible Firmware Interface (UEFI) replaces legacy BIOS as System x's and BladeCenter's new interface between operating systems and platform firmware. UEFI provides a modern, well defined environment for booting an operating system and running pre-boot applications. Unified Extensible Firmware Interface offers several improvements over legacy BIOS:

- Advanced Settings Utility (ASU) now has more complete coverage of system settings.
- On rack mount servers only, UEFI Settings can be accessed out-of-band via ASU and the Integrated Management Module
- Adapter configuration, such as iSCSI, is now in F1 Setup
- Simpler to maintain compatibility with peripherals and system components.
- Elimination of Beep Codes – All errors are covered by Light Path.
- DOS tools are no longer supported.

1.9 What's New – Field Programmable Gate Array (FPGA)

The Field Programmable Gate Array (FPGA) is a device included in high performance systems (such as x3650 X5, x3850 X5, BladeCenter HX5 and others) that acts as a System Control Unit. This component provides the following functionality:

- Power sequencing between multiple planars and/or systems
- System reset control
- Hardware presence and fault detection
- Emergency control
- Communication path between multiple systems and/or memory drawers

Scalable system servers and memory expansion units may contain between 1 and 3 FPGAs in a system. These FPGAs can communicate with other FPGAs in a memory drawer or in other nodes when connected through scalability cables. Any FPGAs that communicate with each other must be at the same firmware level regardless of whether they are in the same system.

2 Requirements for updating firmware

2.1 Important notes

Minimum AMM firmware levels (BladeCenter only)

AMM firmware Version 2.48D (Build ID BPET48D) or higher is required to support HS22.

AMM firmware Version 2.54D (Build ID BPET54D) or higher is required for HS22V blades.

AMM firmware Version 2.54G (Build ID BPET54G) or higher is required for HX5 blades.

Required configuration to enable inband updates

To enable updating via UXSPI, BoMC, or individual update packages, the LAN over USB interface must be enabled. These methods are considered “inband” update methods, and all use the LAN over USB connection to communicate from the operating system to the IMM.

To enable the LAN over USB interface on a rack server, ensure that in the UEFI menu, the option "Commands on USB interface" is enabled (default setting). This can be found in the UEFI menu: Systems Settings → Integrated Management Module → Commands on USB Interface Preference → Commands on USB interface. You can also enable it via the menu in the IMM web interface. Go to System → IMM Control → System Settings, and at the bottom of the page in the Miscellaneous section, ensure that Allow commands on USB interface is set to Enabled.

To enable the LAN over USB interface on a blade server, from the AMM web interface, click on the “Configuration” link under “Blade Tasks”. Scroll down and click on the “Advanced Blade Policy Settings” link at the bottom of the page. Under the “Service Processor's Ethernet over USB interface” section, ensure the status is “Enabled”. If any are disabled, select the checkbox next to the disabled blade(s), and press the “Enable” button. This can also be done using the AMM “ethoverusb” CLI command.

Requirements for updating scalable systems

Review the following important considerations for updating firmware on a scalable system:

- Before connecting 2 systems together with a QPI cable kit to form a scalable complex, you must ensure the UEFI, IMM, FPGA, and DSA preboot firmware levels on both systems are at the same level and are at least at the following minimum levels. You can use ToolsCenter UXSPI or BoMC to display the installed firmware levels and install updates on each system (see section 2.2). After updating the firmware on each system, follow the Installation Instructions that came with your Scalability Kit to connect the systems together.
  - UEFI version 1.23
  - IMM version 1.15
  - FPGA version 1.01
  - DSA preboot version 3.13
- Before connecting a MAX5 to your system with a QPI cable kit, you must ensure the UEFI, IMM, FPGA, and DSA preboot firmware levels are at least at the following minimum levels. You can use ToolsCenter UXSPI or BoMC to display the installed

firmware levels and install updates on each system (see section 2.2). After updating the firmware, follow the Installation Instructions that came with your Scalability Kit to connect the MAX5.
    - UEFI version 1.23
    - IMM version 1.15
    - FPGA version 1.01
    - DSA preboot version 3.13
- It is very important that the firmware levels on all of the servers in a scalable complex be at the same level. Running different levels of firmware on the primary and secondary servers in a scalable complex can lead to unpredictable results. The recommended method for updating the firmware is to use ToolsCenter UXSPI or BoMC . Those update methods will update all of the systems in a scalable complex at the same time. Out of band updates via the IMM or AMM (for the HX5) are supported, however, you must ensure that the firmware for all of the servers in the complex have been updated successfully before rebooting the system. It is imperative to update both servers in a scalable complex together to ensure they're at the same code levels.
- The HX5 blade supports creating a scalable blade complex with the blade servers configured as two independent partitions. In this configuration, the online update utilities can only update the firmware for the partition they are executed on. Due to this, you must update the firmware for each blade independently before rebooting either system. See section 2.5 for details.
- Use caution when attaching or removing QPI cables, as they are fragile. Also, AC power must be off before attaching or removing QPI cables. See the Installation Instructions that came with your Scalability Kit for more information.
- On systems that contain an FPGA, a power off/on cycle is required to activate the new firmware. If the update is performed via an out-of-band method (such as the IMM web interface or AMM web interface) while the system is powered off, the FPGA will be activated immediately. If the update is performed while the system is powered on, the IMM will automatically cycle power to the system at the next reboot to activate the FPGA firmware.

Important notices for updating from any level of IMM firmware prior to 1.15

Review the following important considerations before updating from any level of IMM firmware prior to 1.15:

- Beginning with IMM firmware version 1.15, a DHCP server is included in the IMM to provide an IP address for the internal LAN over USB interface. On a scalable complex, an IP address will be assigned to both of the LAN over USB interfaces. DHCP should be enabled on these interfaces in the operating system to enable updating firmware.
- Windows assigns a 169.254.xxx.xxx address to any interface in the system that is configured for DHCP but cannot reach a DHCP server. If any LAN interface besides the LAN over USB interface is assigned a 169.254.xxx.xxx address, it will prevent the firmware update from completing. Assign an address or disable the interface.
- When updating the IMM firmware from a version earlier than version 1.05 (build YUOO32F) to version 1.05 or newer, the Remote Alert Recipient Email Addresses and the Daylight Saving Time setting will revert to the default setting. Users that utilize these settings will need to set them again after the update.

Other firmware update considerations

- When updating with BoMC, UXSPI, AMM, or in-band via individual update packages, the update will take at least 17 minutes.

- Due to an Intel erratum, if your server is running Linux or VMware, you should disable C-States before you update UEFI, IMM, FPGA, or DSA Preboot. C-states can be returned to the original settings after the updates are complete. See RETAIN TIP H195678 for more information. Updates performed through the AMM, Bootable Media Creator, or the IMM Web or CLI interfaces do not have this requirement.
- If your server has advanced management module (AMM) level 50G or earlier and you will be updating multiple blades in the chassis, restart the AMM once before beginning multiple updates.
- It is recommended that all firmware including IMM, UEFI, FPGA and DSA Preboot are updated together as a matched set. The best practice is to use the UpdateXpress System Pack (UXSP) for a system.
- If a firmware fails to update, the best practice is to reattempt the firmware update before rebooting the system.
- Updated firmware version numbers might not be visible in SMBIOS tables until after the server is rebooted. To verify firmware levels, use UXSPI, BoMC, or ToolsCenter Dynamic System Analysis (DSA).
- The IMM must be reset after updating its firmware before configuration changes can be made. Note that when updating via UXSPI, BoMC, AMM, or individual update packages, the IMM will automatically be reset after updating its firmware (except when updating a scalable system—see section 2.5). If you are updating via IMM, you will need to reset the IMM via the IMM web interface or IMM command line interface.
- After doing a UEFI update you will need to reboot to update the CRTM and activate the new version of UEFI firmware. Recommended best practice after a UEFI update is to reboot the system to allow CRTM to be updated before powering it off for any reason.
- Do not power off the system while the CRTM is being updated; doing so will corrupt the system and require a system board replacement. During the CRTM update, newer versions of UEFI will display the message “Warning: Secure Region Update in Progress, Do Not Power Off System”. Older versions of UEFI will not display the message. After the CRTM is complete, the system will reboot. When you see the IBM UEFI splash screen, it is safe to power off the system.
- When updating UEFI, the system must be powered on, either to a UEFI F1 menu (if updating out of band), or to an operating system (if updating inband).

2.2 Requirements for updating firmware via ToolsCenter UpdateXpress System Pack Installer (UXSPI) or ToolsCenter Bootable Media Creator (BoMC)

ToolsCenter Bootable Media Creator (BoMC)

- If the BoMC .ISO image that is created will be remote mounted via the IMM remote control, some servers may require a remote access feature key to utilize that functionality.
- If you are flashing the server via IMM’s remote control, you will lose your session when the IMM is being rebooted after flashing.
- 8677 BladeCenter – E (1xx, 2xx and 3xx --non-refresh models) may require an HS22/HS22V USB port speed configuration change. See RETAIN Tip H163233 for details.
- The LAN over USB interface must be enabled. See Required configuration to enable inband updates for instructions on how to enable it.

- Best practice is to use the latest level of BoMC to flash your system.

ToolsCenter UpdateXpress System Pack Installer (UXSPI) and individual update packages

- Requires an operating system to be installed on the server prior to execution of the package.
- The LAN over USB interface must be enabled. See Required configuration to enable inband updates for instructions on how to enable it.
- Requires the device driver for the LAN over USB interface to be installed and configured.
- Best practice is to use the latest level of UXSPI to flash your system.

Notes

- The online firmware update utilities use the Ethernet (LAN) over USB interface to communicate with the IMM. BoMC and UXSPI will automatically enable and configure this interface.
- For VMWARE 4.x, you must execute the following command to disable the firewall:
  - `esxcfg-firewall -o 623,udp,out,USBLan`
- If VMware was installed with the LAN over USB interface disabled, the OS will react to it being enabled by adding it to a new virtual switch. It is advised to configure the system to co-exist this new network with the existing external LAN so that future updates will be non-disruptive.
- Dynamic System Analysis (DSA) Preboot version 2.33 requires Integrated Management Module (IMM) firmware version 1.05 or newer.
- When updating via UXSPI, the Broadcom NetXtreme II device driver must be at or above the following levels:
  - Windows --NDIS 4.6.15; VBD 4.6.17
  - Linux-- 1.8.2b
  - VMware 3.5 --Update 5
  - VMware 4.0 -- Version 2.0.7c
- When updating a scalable blade complex configured as independent partitions, you must follow the following procedure
  - Execute UXSPI or BoMC on the primary system. Do not reboot the system.
  - Execute UXSPI or BoMC on the secondary system.
  - Reboot both systems.

  If the scalable blade complex is configured as a single partition, UXSPI and BoMC will update both servers at the same time.

2.3 Requirements for updating IMM, UEFI, FPGA, and DSA preboot firmware via individual update packages

The recommended way to update firmware is to use to use ToolsCenter UpdateXpress System Pack Installer (UXSPI) or Bootable Media Creator (BoMC) (see section 2.2). If you choose to update your firmware via individual packages, the preferred order to update the firmware is:

- Integrated Management Module (IMM)
- UEFI firmware
- FPGA firmware (if applicable to the system)

- Dynamic System Analysis (DSA) Preboot

This order applies regardless of whether you run the individual update packages manually, or script them to run inband or out of band (via the IMM or AMM).

Note: When comparing the preferred order shown above, to the order UXSPI or BoMC perform the updates, you may find differences. The tools determine the correct and optimal order to apply the updates based on information available in the associated XML files and code levels currently installed on the system.

Note: Applying individual update packages inband requires the device driver for the LAN over USB interface to be installed and configured.

Note: After applying the IMM firmware update, the IMM will be reset. The initial restart after updating the IMM firmware can take up to 20 minutes. If you run the individual update packages inband, they will automatically delay the correct amount of time. If you use an out of band method, ensure your scripts are prepared to wait this amount of time before starting the next update to ensure successful updates.

2.4 Requirements for updating IMM and UEFI firmware via the AMM (BladeCenter only)

- When updating IMM and UEFI firmware via the AMM Command Line Interface (Telnet/SSH), set the inactivity timer to zero (0) during the update process. Run the following command after logging in via Telnet/SSH:

  ```
  telnetcfg -t 0 -T system:mm[1]
  ```

  where 1 is the active advanced management module bay. After the update completes, reset the timer to the previous value.
- Ensure that all blades have been discovered and VPD is correctly displayed with no errors in the AMM event log.
- The management network must be operational on the blade. To view the status of the management network, log into the AMM, and then navigate to Blade tasks → Power / restart.
- For the management network to be operational, you must either have an Ethernet switch installed in I/O bay 1 of the BladeCenter chassis or enable MCAD.
  - The Copper Pass-thru Module (CPM) and Optical Pass-thru Module (OPM) do not support updating IMM, UEFI, or FPGA firmware. If you have one of these installed in I/O bay 1, you must enable MCAD (see below).
  - When using an Intelligent Copper Pass-Thru Module (iCPM), the external port of the iCPM that corresponds to the blade that is being updated must be connected and have a link to an upstream switch.
  - No special configuration is needed when using the Ethernet switches at default settings.
  - Ensure VLAN 4095 is enabled (this is default).
- If no switches are present in bay 1, you must have a switch in I/O bay 2, 3, 4, 7, 8, 9, or 10, and enable MCAD. To enable MCAD:
  - Navigate to Blade Tasks → Configuration → Management Network. Ensure VLAN 4095 is enabled (this is default). Ensure “Enable Management network auto-discovery” is checked.
  - Click Save.
- On the blade, you must have an Ethernet link to an I/O bay using either the on-board or the added adapter. Note that on the blade, if network teaming is configured, it can prevent the management network from functioning.

- The AMM TFTP server must be enabled.
  - This can be done under MM Control – Network Protocols or Command Line (ports -tftpe on)
- The blade should not be rebooted during the update process.
- The UEFI should only be updated via the AMM when the blade is:
  - Powered on with the operating system fully loaded.
  - At the F1 setup screen but not at a UEFI submenu.
- Note that DSA Preboot cannot be updated via the AMM. Use ToolsCenter UpdateXpress System Pack Installer (UXSPI) or ToolsCenter Bootable Media Creator (BoMC) to update the DSA Preboot firmware.
- Note: The BladeCenter HX5 Problem Determination and Service Guide contains an example script for updating firmware via the AMM CLI.

2.5 Required procedures for updating firmware of a scalable system via individual update packages

Note: For definitions of the terms "Partition" and "Scalable complex", please see the user's guide for the x3850 X5, x3950 X5, x3690 X5, or BladeCenter HX5. See Section 4, Additional Information for links

The recommended way to update firmware is to use to use ToolsCenter UpdateXpress System Pack Installer (UXSPI) or Bootable Media Creator (BoMC) (see section 2.2). If you choose to update your firmware via individual packages, you must make sure that you update the firmware for each server in the scalable complex to the same levels before resetting the complex. Refer to the following table to select the correct procedure to follow based on your configuration and preferred update method:

	Inband update method	**Out of band update method**
Single partition ("merged" configuration)	Procedure 1	Procedure 2
Independent partitions	Procedure 2	Procedure 2

2.5.1.1 Procedure 1

In this scenario, you are updating firmware on a scalable complex configured as a single partition running individual update packages inband on an installed operating system.

The recommended procedure to update the firmware is:

1. Run the IMM firmware update package on the system.
2. Run the UEFI firmware update package on the system
3. Run the FPGA firmware update package on the system
4. Run the DSA preboot firmware update package on the system
5. Reboot the system to activate the firmware

Note: In this scenario, each firmware update package will automatically update the firmware on both the primary and secondary systems when they are invoked.

2.5.1.2 Procedure 2

In this scenario, updates must be applied to each system in the scalable complex independently.

1. Update the IMM firmware on the primary system and then the secondary system
2. Reset the IMM on the primary and secondary systems. See below for instructions on how to do this via the IMM and AMM web interface.
3. Update the UEFI firmware on the primary system and then the secondary system

4. Update the FPGA firmware on the primary system and then the secondary system
5. Update the DSA preboot firmware on the primary system and then the secondary system
6. Reboot both servers to activate the firmware

2.5.1.2.1 Resetting the IMM via the IMM web interface

1. Select “Restart IMM” underneath “System/IMM Control” in the navigation tree on the left side.
2. Click the “Restart” button.

2.5.1.2.2 Resetting the IMM via the AMM web interface

1. Select the “Power/Restart” task underneath the “Blade Tasks” in the navigation tree on the left side.
2. On this page, select the checkbox next to the blades to be reset.
3. In the “Available actions” drop down list, select “Restart Blade System Mgmt Processor” and click the “Perform Action” button.

3 RETAIN Tips

3.1 Applicable to IMM-based blade and rack-mount systems

General

- H194823 BOOTABLE FIRMWARE UPDATES FOR IMM BASED SYSTEMS
- H195678 IMM/UEFI FLASH FAILS RUNNING LINUX
- H195926 SERVERAID MR10I CONTROLLER CAUSES UNEXPECTED SYSTEM HANGS
- H195999 DSA PREBOOT 2.33 FAILS TO FLASH ON SYSTEMS WITH IMM
- H196283 VMWARE - ERROR FLASHING FIRMWARE: 3

UEFI

- H196258 UEFI UPDATE UNSUCCESSFUL DUE TO MINIMUM LEVEL CHECK FAILURE
- H196209 UPDATING UEFI BACKUP FIRMWARE WITH IMM32F MAY FAIL
- H195678 IMM/UEFI IMM/UEFI FLASH FAILS RUNNING LINUX
- H196270 SYSTEM IS UNABLE TO UPDATE UEFI UNDER SLES11

IMM

- H195915 REMOTE CONTROL VIDEO DISAPPEARS AFTER IMM FIRMWARE UPDATE
- H196008 IMM CONFIGURATION SETTINGS NOT SAVED WHEN FW IS DOWNGRADED
- H194793 SERVER APPEARS SLOW TO ACCEPT POWER ON/IMM COMMUNICATIONS
- H194971 AVOIDING CONFLICTS WITH OPEN MPI
- H195968 IMM 19E REQUIRES REBOOT IF VPD IS CHANGED PRIOR TO FLASHING
- H196052 ALERT AND DST CHANGED AFTER FLASHING UP FROM IMM 23C/24I
- H197152 Multinode Power On Not Responsive Right After Power Off
- H197140 X5: System Restart Cause May Confuse Users
- H197117 Uploading a Floppy Image Not Removed Until Unloaded
- H196762 X3850 X5/X3950 X5: Boots To Back Up UEFI
- H197111 Cancelling RDOC Load In IMM Does Not Cancel Upload
- H197134 Error Flashing FPGA - Error Getting Build ID
- H197115 X3850 X5: Fan Tach and Device Numbers Do Not Match
- H197186 Intermittent Uncorrectable Bus Errors At Post
- H197658 SNMP firmware update fails with partial image transfer error - IBM System x3690 X5, x3850 X5, x3950 X5

3.2 Applicable only to IMM-based rack-mount systems

General

- H196329 FRONT PANEL NMI RECOVERS, BUT SYSTEM HEALTH STILL CRITICAL

UEFI

- H195011 IMM CLI CALLS FOR A REBOOT IMM AFTER UEFI FLASH

IMM

- H195023 FLASHING FIRMWARE FROM IMM CLI, EVENT LOG MSG IS INCOMPLETE

3.3 Applicable only to IMM-based blades

UEFI

- H197034 HS22 HANGS AT "UEFI PLATFORM INITIALIZATION" AFTER BACKFLASH
- H195984 BLADE MAY NOT BE ABLE TO FLASH FIRMWARE WITHIN OPERATION SYSTEM

4 Additional Information

- ToolsCenter Bootable Media Creator (BoMC)
  - http://www.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=TOOL-BOMC&brandind=5000016
- ToolsCenter UpdateXpress System Pack Installer (UXSPI)
  - http://www.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=SERV-XPRESS&brandind=5000016#uxspinstall
- ToolsCenter Dynamic System Analysis (DSA)
  - http://www.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=SERV-DSA&brandind=5000016
- User's Guide for Integrated Management Module (Includes error messages)
  - http://www.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-5079770&brandind=5000008
- BladeCenter Advanced Management Module Command-Line Interface Reference Guide
  - http://publib.boulder.ibm.com/infocenter/bladectr/documentation/index.jsp?topic=/com.ibm.bladecenter.advmgtmod.doc/adv_mgt_mod_cli_guide.html
- Product documentation for BladeCenter blade servers
  - http://publib.boulder.ibm.com/infocenter/bladectr/documentation/index.jsp?topic=/com.ibm.bladecenter.common.nav.doc/bc_servers_welcome_page.html
- IBM BladeCenter HX5 Problem Determination and Service Guide
  - http://publib.boulder.ibm.com/infocenter/bladectr/documentation/index.jsp?topic=/com.ibm.bladecenter.hx5.doc/dw1it_r_printable_doc.html
- Installation and User's Guide - IBM BladeCenter HX5
  - http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5084612
- Installation and user's guide - System x3850 X5, System x3950 X5
  - http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5085479
- Installation and User's Guide - IBM System x3690 X5
  - http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5085206
- White Paper: Life Without DOS, Transitioning to UEFI and IMM
  - http://www.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-5079769&brandind=5000008
- IBM BladeCenter HS22 Technical Introduction IBM RedPaper
  - http://www.redbooks.ibm.com/abstracts/redp4538.html