IBM FlashSystem® 900

Firmware Version 1.6.1.5

Release Date: October 31, 2022

Contents

Applicable systems
Product resources
Bug severity legend
Latest changes
- Latest fixes
- Remediated security vulnerabilities
- Release features
- Known issues

Currently supported specifications
Release history
Upgrading firmware
- Release overview
- Supported upgrade paths
- Preparing to upgrade
- Performing the upgrade
- Troubleshooting

Contact information
Revision history
Copyright notice

Applicable systems

This release is only supported for the following products:

- IBM FlashSystem 900, MTMs 9840-AE2 and 9843-AE2
- IBM FlashSystem 900, MTMs 9840-AE3 and 9843-AE3
- IBM FlashSystem 900, MTM 9843-UF3

Note: FlashSystem 840 (AE1 model) systems are not supported at 1.6 and later code levels. In addition, support for systems using iSCSI or FCoE is no longer available in 1.5 releases and later.

Product resources

IBM FlashSystem 900 product resources guide users through the various features and components of the storage system, including usage and troubleshooting guides. To read about this storage system and learn how to use or troubleshoot, see IBM Documentation for IBM FlashSystem 900 or visit the IBM Redbooks® website for the IBM FlashSystem 900 Product Guide.

Bug severity legend

The following explains the bug severity ranking used for key fixes and in the Release history:

Severity	Description
S1	Recommended upgrade for all users as soon as possible.
S2	Recommended upgrade for all users at the next scheduled maintenance window
S3	Recommended upgrade at the next scheduled maintenance window only for users experiencing the issue. All others may consider this to be an S4.
S4	Upgrade at the next scheduled maintenance window. May be performed at the discretion of the user if the issue is having a negative impact.
S5	Upgrade is not necessary. This would include a mostly cosmetic or minor annoyance fix.

Latest changes

The current release is a Program Temporary Fix (PTF) for IBM FlashSystem 900 customers and includes a security remediation.

After initial configuration of the hardware is complete, IBM strongly recommends that you make sure that your IBM FlashSystem firmware is up-to-date. Visit IBM Fix Central using the link below to see if any updates are available for your system.

Latest fixes

Return to top

Available firmware releases are listed on IBM Fix Central. For issue severity definitions, see the Bug severity legend.

Remediated security vulnerabilities

The following security vulnerability has been remediated in this release:

FLASH-29806: (CVE-2021-35603, CVE-2021-35550) An unspecified vulnerability in Java SE related to the JSSE component could allow an unauthenticated attacker to obtain sensitive information resulting in a low confidentiality impact using unknown attack vectors. For more information on this vulnerability, see the following IBM security bulletin: Security Bulletin: Vulnerabilities in IBM Java affect IBM FlashSystem models FS900 and V9000

FLASH-29809: (CVE-2022-0778) OpenSSL is vulnerable to a denial of service, caused by a flaw in the BN_mod_sqrt() function when parsing certificates. By using a specially-crafted certificate with invalid explicit curve parameters, a remote attacker could exploit this vulnerability to cause an infinite loop, and results in a denial of service condition. For more information on this vulnerability, see the following IBM security bulletin: Security Bulletin: Vulnerability in OpenSSL affects IBM FlashSystem models FS900 and V9000

Release features

The following information lists the features that come with the 1.6 release of IBM FlashSystem 900 product.

1.6 features

The following are features of all 1.6 releases and are therefore included in the latest release:

- New hardware - 40 TB flash modules and 4x16 Gb NVMe/Fibre Channel (FC) Adapters are introduced with 1.6.0.0.
- NVMe (Non-Volatile Memory Express) over FC - Starting in 1.6.0.0, NVMe is available for use with FC systems.
- IBM SKLM version 3 - Version 3 of SKLM is supported starting in 1.6.1.0.
- Domain Name System (DNS) for LDAP - Common names can be assigned to LDAP servers using DNS starting in 1.6.1.0.
- Improved Rebuild Speeds - Array rebuilds for AE3 flash modules are improved starting with 1.6.1.0.
- Remote Code Load - Systems can be upgraded remotely by IBM Support.
- Security - Systems initialized at the 1.6.1.1 code level will require that the default system password be changed before full use of the system is unlocked.

1.5 features

The following are features of all 1.5 releases and are therefore included in the latest release:

- Remote Support Assistance - IBM Support can now access user systems remotely and provide assistance via the command line if this feature is enabled.
- IBM Security Key Lifecycle Manager (SKLM) - Encryption can be enabled using SKLM, which provides access to system encryption keys using servers.
- Open PMR - Users can now raise events from the user management GUI against their system. This event triggers a Problem Management Record (PMR) to be opened. The user can provide a short description of the perceived issue and IBM support will be notified. This feature is available from the **Monitoring** --> **Events** panel or from the banner help drop down menu anywhere in the GUI.
- Environmental improvements have been made which provide better system hardware stability.
- Systems that support flash modules with compression hardware will now allow users to utilize more logical space than there is physical capacity through compression.
- RESTful API - Hardware health check has been updated to include upgrade status and compression information has been added for the array.
- NVMe over IB (InfiniBand) - Starting with release 1.5.1.0, NVMe is available for use with IB systems only.
- Provide Feedback - Customers can now provide feedback via the user management GUI 90 days after installation.
- IBM Spectrum Control Storage Insights Foundation - In version 1.5.2.1, system event log information is available through this portal, which allows users to view and monitor their Storage Systems.

1.4 features

The following are features of all 1.4 releases and are therefore included in the latest release:

- Test Only utility - A **Test Only** button has been added to the GUI for the update test utility. Users can now test their systems for issues that might hinder an upgrade without starting the upgrade. This button is found by navigating to Settings System Update System.
- Default logout time - A logout time can now be set under **Settings** --> **GUI preferences** --> **General**. The default logout time is set to 120 minutes. This can either be increased, decreased, or disabled.
- Login message - Users can configure a login message which appears under the authentication fields for the GUI login.

- SSL certificate panel - Secure Communications is enhanced with the new SSL certificate panel in the GUI, found by navigating to **Settings** --> **Security** --> **Secure Communications**.
- RESTful API - System health check added and battery reconditioning added.
- Automatic battery reconditioning - Starting in 1.4.7.0 firmware, if automatic battery reconditioning is turned on, battery reconditioning will automatically start for a redundant battery if needed.

1.3 features

The following are features of all 1.3 releases and are therefore included in the latest release:

- Sector size support on VDisk creation through the GUI
- Interface quality improvements
- The multi-system monitoring GUI tool Neighborhood has been re-enabled.
- Upgrade test utility improvements.

1.2 features

The following are features of all 1.2 releases and are therefore included in the latest release:

- Error isolation and detection logic throughout data path to enhance component failure identification
- Integrity is ensured with the addition of a background continuous array sweeper.
- The ability to correct certain single drive errors from system level RAID which serves to reduce the need for flash module replacement
- Background trim functions to reclaim unused space.
- Support for SCSI UNMAP.
- Support for the VMware vSphere Storage APIs Array Integration (VAAI) UNMAP action.
- The first 1MB of VDisk space is deleted upon creation to remove any old file system information.
- Support for VMware vSphere API for Storage Awareness (VASA).
- Support for a RESTful API.
- Rear system view of components is available through the management GUI.
- The multi-system monitoring tool called Neighborhood is available for use through the GUI.

Known issues

Users with virtualized storage on SVC versions 8.1.0.2 or 8.1.1.0 who are considering upgrading to 8.1.1.1 *must* update using special instructions detailed here. See Fix Central for these releases.

Beginning with release 1.6.1.0, when using a fully qualified domain name or DNS shortname containing a "_" (underscore), a blank page or http error 400 is displayed while attempting to launch the management GUI. This change complies with the RFC1035 specification for domain names. See this article for details.

To stay up-to-date on current known issues, workarounds, downloads, and other documentation from support, please ensure that you have subscribed to My Notifications.

Currently supported specifications

Protocol	Description
SCSI-SAM-3	SCSI Architecture Model (v3)
SCSI-SPC-3	SCSI Primary Commands (V3)
SCSI-SBC-2	SCSI Block Commands (V2)
SCSI-FCP-3	Fibre Channel (FC) Protocol (V3)
SCSI-SRP	SCSI RDMA Protocol
FC-PH-3	FC Physical and Signaling Interface (V3)
FC-AL-3	FC Arbitrated Loop (V2)
IBTA-1.2	InfiniBand (IB) Trade Association Architecture Specification (V1.2)
NVMe-1.3.0	NVMe over Fabrics 1.0 (which includes the RDMA/IB mapping). NVMeoFC Rev 1.19 & AM1

Return to top

Note: To test or demonstrate concurrent maintenance on canisters and batteries, use this featured document, which describes the recommended process for concurrent maintenance.

Release history

The following sections include a list of all fixes and improvements for previous FlashSystem 900 releases.

Release 1.6.1.4

Release Date: October 20, 2021

The following issues were fixed in release 1.6.1.4:

FLASH-29791: A vulnerability (CVE-2021-29873) in the IBM FlashSystem restricted shell has been remediated. For more information on this vulnerability, see the following IBM security bulletin: Security Bulletin: A vulnerability exists in the restricted shell of the IBM FlashSystem 900

Release 1.6.1.3

Release Date: April 13, 2021

The following issues were fixed in release 1.6.1.3:

FLASH-29756 - Add data integrity protection between the PCIe link to the HBA and the DDR memory. (S1)

FLASH-29749 - Prevent unnecessary flash module failures when upgrading from 1.5.2.8 on AE2 systems. (S2)

FLASH-29729 - Prevent certain error conditions from faulting AE2 flash modules. (S2)

FLASH-29739 - Weak DSA host keys should not be allowed. (S4)

Vulnerabilities in Java (CVE-2020-14579, CVE-2020-14578, CVE-2020-14577), and CVE-2020-2781 have been remediated in this release. For more information on these vulnerabilities, see the following IBM security bulletins: Security Bulletin: A vulnerability in Java affects the IBM FlashSystem 900 (CVE-2020-2781) and Security Bulletin: Vulnerabilities in Java affect the IBM FlashSystem 900 (CVE-2020-14577, CVE-2020-14578, CVE-2020-14579)).

A vulnerability in Tomcat (CVE-2020-13935) has been remediated in this release. For more information on this vulnerability, see the following IBM security bulletin: Security Bulletin: A vulnerability in Tomcat affects the IBM FlashSystem 900 (CVE-2020-13935).

A vulnerability (CVE-2020-4987) in the management GUI of the IBM FlashSystem 900 has been remediated in this release. For more information on this vulnerability, see the following IBM security bulletin: Security Bulletin: A vulnerability exists in the management GUI of the IBM FlashSystem 900

Release 1.6.1.2

Release Date: May 26, 2020

The following issues were fixed in release 1.6.1.2:

FLASH-29637 - A mitigation was added for the interface controllers to prevent system outages due to internal hardware failure. (S1)

FLASH-29640 - An "invalid" health reading should not fail a flash module. (S2)

FLASH-29628 - Pulling Fibre Channel (FC) cables on AE3 systems with 4x16 Gb NVMe/FC adapters could cause longer than expected recovery times. (S3)

FLASH-29591 - NVMe over FC support is needed for RHEL 8.1 and SLES 15 SP2 Operating System versions. (S3)

Vulnerabilities in Java (CVE-2019-2989 and CVE-2019-2964) have been remediated in this release. For more information on these vulnerabilities, see IBM's security bulletin: Security Bulletin: Vulnerabilities in Java affect the IBM FlashSystem 900 (CVE-2019-2989 and CVE-2019-2964)

Release 1.6.1.1

Release Date: November 11, 2019

Return to top

The following issues were fixed in release 1.6.1.1:

FLASH-28268 - Collecting flash module LED status should not cause a node failover to stall. (S1)

FLASH-29113 - Improve error recovery handling in rare data loss during a loss of access event. (S1)

FLASH-29384 - Aborted Non-volatile Memory express (NVMe) over Fabrics commands may overwrite the data transfer buffer of another command, including other Small Computer System Interface (SCSI) commands. (S1)

FLASH-29263 - On Fibre Channel (FC) connections with both FC and NVMe over FC connections, process login types were not properly validated. (S1)

FLASH-29003 - Fix the sector size reporting for volumes advertised using NVMe over FC which previously always reported a size of 512 bytes. (S3)

FLASH-29272 - Link instability on direct attached link up can lead to login stalls. (S4)

FLASH-28630 - Increase cable pull resiliency for NVMe/FC adapters. (S4)

FLASH-29228 - NVMe over FC interface controllers now support up to 512 associations. (S5)

FLASH-29203, 28742 - Fix minor NVMe over FC protocol issues. (S5)

FLASH-29042 - Fix packet length of NVMe over FC process login response payload. (S5)

FLASH-29146 - Remediate multiple vulnerabilities in the Linux kernel which affect IBM FlashSystem 900 (CVE-2019-11479, CVE-2019-11478, and CVE-2019-11477). More information is available on these vulnerabilities through the following security bulletin:

Security Bulletin: Multiple Vulnerabilities in the Linux kernel affect the IBM FlashSystem models 840 and 900

FLASH-29207 - Remediate a vulnerability in HTTP which affects IBM FlashSystem 900.

Release 1.6.1.0

Release Date: June 28, 2019

The following issues were fixed in release 1.6.1.0:

FLASH-29023 - After one system battery is successfully replaced, replacing the second battery will cause it to come up in a degraded state. (S2)

FLASH-28505 - Rare timing condition can cause a loss of access after a flash module communication error. (S2)

FLASH-26930 - Internal communication errors could cause an interface controller to be unable to perform RAID reconstruct and validation operations until reset. (S2)

FLASH-28280 - Collection of support logs or failure of a system component during a system upgrade could cause the upgrade to stall with a possible loss of access. (S2)

FLASH-28833 - The event with ID 085081 and description "Array storage is critically low on available physical space" should not be able to be manually marked as fixed. (S4)

FLASH-28722 - Rules for creating NVMe-FC hosts should not include case sensitivity. (S4)

FLASH-27063 - NVMe-FC systems should be allowed to connect to Windows hosts. (S4)

FLASH-28793 - Minor issues with LDAP management GUI panel. (S5)

FLASH-28685 - CLI output for the lsarray command should not include a value for "effective used capacity" on systems with models AE1 or AE2. (S5)

FLASH-28351 - The event with ID 988011 and description "Array storage is low on available space" should be able to be manually marked as fixed. (S5)

FLASH-28683 - The management GUI dashboard includes an inaccurate Japanese translation for the word "ratio." (S5)

FLASH-28051 - Upload folder does not yield directory pop up on management GUI System Update page when using Chrome browser. (S5)

FLASH-27725 - Some label stats are showing "undefined" on the management GUI performance page when creating custom charts. (S5)

FLASH-27076 - Fast array validation tool cannot be turned off while in progress. (S5)

Return to top

FLASH-28611, 27717, 26996, 26556 - Remediate multiple vulnerabilities in Java which affect IBM FlashSystem 900 (CVE-2018-12547, CVE-2018-2180, CVE-2018-1517, and CVE-2018-2783). More information is available on these vulnerabilities through this link: Security Bulletin: Multiple Vulnerabilities in Java affect IBM FlashSystem 840 and 900

FLASH-29146 - Remediate a vulnerability in Java which affects IBM FlashSystem 900 (CVE-2019-2602). More information is available on these vulnerabilities through this link: Security Bulletin: A vulnerability in Java affects IBM FlashSystem 840 and 900

FLASH-27878 - Remediate a vulnerability in IBM FlashSystem 900 service assistant GUI. (S4)

FLASH-27479 - Remediate a vulnerability in Apache Tomcat which affects IBM FlashSystem 900 (CVE-2018-11784). More information is available on these vulnerabilities through this link: Security Bulletin: A vulnerability in Apache Tomcat affects IBM FlashSystem 840 and 900

FLASH-27632 - Remediate a vulnerability in OpenSLP which affects IBM FlashSystem 900 (CVE-2017-17833). More information is available on these vulnerabilities through this link: Security Bulletin: A vulnerability in OpenSLP affects IBM FlashSystem 840 and 900

Security Bulletin: Multiple Vulnerabilities in the Linux kernel affect IBM FlashSystem 840 and 900

Release 1.6.0.1

Release Date: April 16, 2019

The following issues were fixed in release 1.6.0.1:

FLASH-28538 - AE3 systems upgraded to 1.6.0.0 from 1.5.0.0 - 1.5.2.4 firmware versions will not have additional compression space management functionality initialized, which makes it more difficult for a system that runs out of space to be properly cleaned enough to exit WRITE PROTECT mode. (S1)

FLASH-28583 - HIPER (Highly Pervasive): Abort handling on NVMe-FC connections could result in multiple host commands sharing the same transfer buffer, which can lead to data errors. This issue only applies to NVMe-FC adapters. (S1)

FLASH-28584 - Fix issue with NVMe-FC where failed operations could report incorrect status to the host, potentially reporting good status for failed commands. This issue only applies to NVMe-FC adapters. (S1)

FLASH-28582 - Removal of a physical interface cable on NVMe-FC systems could result in that adapter no longer servicing host commands. This issue only applies to NVMe-FC adapters. (S2)

FLASH-27034 - Reduce chance for power spike on flash modules. (S3)

Release 1.6.0.0

Release Date: February 26, 2019

The following issues were fixed in release 1.6.0.0:

FLASH-24962 - Fix issues with canister internal errors sometimes seen on systems with 1.4 firmware. (S3)

FLASH-27058 - Ensure that an Out of Space event will be raised again when appropriate after being marked as fixed. (S3)

FLASH-27209 - Neighborhood view shows an informational event as a system alert. (S4)

FLASH-26913 - Add array used effective capacity to lsarray CLI output. (S4)

FLASH-26882 - Add flash module physical and effective capacity to lsdrive CLI output. (S4)

FLASH-26888 - Improve low and out of space management when a compression-capable enclosure is managed by SVC. (S4)

FLASH-27296 - Several improvements made to GUI storage capacity displays. (S5)

FLASH-27260 - Several improvements made to GUI progress indicators. (S5)

FLASH-27209 - Neighborhood view shows an informational event as a system alert. (S5)

FLASH-27097 - GUI performance dashboard should provide guidance to the user on the projected physical capacity usage. (S5)

Return to top

FLASH-26954 - Fix various browser-specific issues with the user management GUI. (S5)

FLASH-26857 - Several improvements made to GUI performance charts. (S5)

FLASH-26622 - Detailed array information needs to be provided in support logs. (S5)

FLASH-24927 - Multiple wording improvements should be made to GUI fix procedures. (S5)

Release 1.5.2.5

Release Date: April 29, 2019

The following issues were fixed in release 1.5.2.5:

FLASH-27558 - Under rare circumstances, stalled commands are not properly recovered which can lead to a loss of access. (S2)

FLASHHW-752 - Flash modules will now always detect corrupted write data before returning status, preventing the possibility of multiple bad data pages on a single RAID stripe. (S3)

FLASH-28653 - "Canister fault type 2" GUI maintenance procedure results in "Unable to proceed." (S3)

FLASH-28163 - Improve data stability for NVMe over IB systems upon link reseat. (S3)

FLASH-28108 - Make potential physical capacity usage of volumes with compression more clear. (S3)

FLASH-27912 - Ensure that an Out of Space event will be raised again when appropriate after being marked as fixed. (S3)

FLASH-28225 - Improve low and out of space management when a compression-capable enclosure is managed by SVC. (S4)

FLASH-26883 - Add flash module physical and effective capacity to the management GUI. (S4)

FLASH-26882 - Add flash module physical and effective capacity to lsdrive CLI output. (S4)

FLASH-27916 - Add array used effective capacity to lsarray CLI output. (S4)

FLASH-27980 - Add support for SSL protocol 4. (S4)

FLASH-28238 - The GUI System export button yields a communication error. (S5)

FLASH-27097 - The GUI performance dashboard should provide guidance to the user on the projected physical capacity usage. (S5)

FLASH-28051 - Clicking the upload folders on the GUI Update System wizard does not yield a Browse pop up for Chrome users. (S5)

FLASH-27491 - Remediate a vulnerability which affects IBM FlashSystem 900 (CVE-2018-1775). More information is available on this vulnerability through the following security bulletin: Security Bulletin: A vulnerability affects the IBM FlashSystem 840 and 900

Release 1.5.2.1

Release Date: October 15, 2018

The following issues were fixed in release 1.5.2.1:

FLASH-26705 - AE3 flash modules may erroneously present to be in low health which will eventually be failed. (S2)

FLASH-26997 - During upgrade or normal operation, reset of hardware communication parameters could cause a flash module to fail. (S2)

FLASH-26068 - In rare cases, AE3 flash modules could decrease in performance. (S3)

FLASH-27034 - Reduce chance for power spike on flash modules. (S3)

Return to top

FLASH-26428 - There is potential for a canister warmstart and failover resulting in an internal error. (S4)

FLASH-26774 - When expanding a VDisk using the GUI, values over 1000 are not allowed. (S4)

FLASH-26274 - Remote support collection of snap may report as failed upon first attempt. (S5)

FLASH-26438 - Collecting logs using the Service Assistant GUI may not allow the user to save the file to their local computer. (S5)
FLASH-26310 - Repeated attempt to collect logs using the Service Assistant GUI may fail. (S5)

⊖ Release 1.5.1.2

Release Date: June 19, 2018

The following issues were fixed in release 1.5.1.2:

FLASH-26370 - Systems with AE1 and AE2 hardware at the 1.5.1 code level will lose array validation and VDisk space reclamation functionality. (S1)

FLASH-26391, 26388, 26117 - Improve timing to prevent erroneous flash module failures which in rare cases can lead to an outage. (S2)

FLASH-26480 - For InfiniBand (IB) systems only, upon upgrading to 1.5.1.0 or 1.5.1.1, system interface ports have assigned default port IP addresses. See Known Issues for more information. (S4)

⊖ Release 1.5.1.1

Release Date: April 23, 2018

The following issues were fixed in release 1.5.1.1:

FLASH-26141, 26098, 26140, 26097, 26136, 25935, 26138, 26137, 26186, 26139- Remediate multiple vulnerabilities which affect IBM FlashSystem 900 including CVE-2018-1433, CVE-2018-1434, CVE-2018-1438, CVE-2018-1461, CVE-2018-1462, CVE-2018-1463, CVE-2018-1464, CVE-2018-1465, CVE-2018-1466, and CVE-2018-1495. More information is available via the following security bulletins:

- Security Bulletin: Multiple vulnerabilities affect the IBM FlashSystem models 840 and 900
- Security Bulletin: A vulnerability affects the IBM FlashSystem models 840 and 900

FLASH-26174 - The GUI fix procedure for battery event 1114 should account for a battery already having completed its hardware update. (S4)

FLASH-26192, 26253 - Reduce superfluous support log messages. (S5)

⊖ Release 1.5.1.0

Release Date: February 21, 2018

The following fixes were included with the release of firmware version 1.5.0.0.

FLASH-23975 - Remediate multiple vulnerabilities in GNU Bash (CVE-2016-0634, CVE-2016-7543, and CVE-2016-9401).

FLASH-24631 - The system should not take into account temperature readings from failed flash modules. (S2)

FLASH-20878 - Improve internal communication to prevent transient errors from failing flash modules. (S2)

FLASH-24121 - Add a retry for transient errors to avoid unnecessary flash module failures. (S2)

FLASH-25493 - Add support for a new security protocol which complies with NIAP guidelines. (S3)

FLASH-24734 - Add a retry for reading Vital Product Data (VPD) to avoid unnecessary 509 node error states. (S3)

FLASH-23384 - Unepected loss of power or reboot can potentially cause a failure to unlock flash modules. (S4)

FLASH-16520 - Network Neighborhood configuration syncing should be more reliable. (S4)

FLASH-24190 - Restarting the web service can result in an internal error on the configuration node canister. (S4)

Return to top

FLASH-23170 - New event and fix procedure needed for an out of space configuration canister SSD. (S5)

FLASH-13514 - Renaming a host does not properly update in some management GUI panels. (S5)

FLASH-4858 - The user management GUI should support assigning a specific Logical Unit Number (LUN) to a VDisk. (S5)

The following is a list of fixed issues from previous 1.5 code versions:

FLASH-25689 - Support packages collected in 1.5.0.0 do not include all relevant information. (S2)

FLASH-25146 - If a rebuild task takes too long, interfaces may not be prompted to perform a reset recovery. (S2)

FLASH-25418 - A hot pull of the configuration node canister could result in failure of interface adapters in the remaining canister. (S2)

FLASH-25651 - Allow special characters in passwords when logging in with the management GUI. (S3)

FLASH-25562 - Users with 1.5.0.0 firmware could log in using a username entered with additional asterisks and the correct password. (S3)

FLASH-25655 - Prevent certain 509 node boot up errors in prior 1.5.0.x firmware levels. (S3)

FLASH-25380 - Remote support assistance configuration may not remain consistent after FRU canister replacement. (S3)

FLASH-25465 - Configuration recovery with SKLM encryption could not finish successfully.< (S3)

FLASH-25053 - Increase number of interface controller rebuild tracking structures by 4 times to prevent running out under extreme cases. (S3)

FLASH-25458 - If a rebuild task takes too long, interfaces may not be prompted to perform a reset recovery.< (S3)

FLASH-25164 - In the very unlikely event of not having enough rebuild tracking structures, the interface controller will now properly return the SCSI BUSY status, which will indicate the command needs to be retried. (S3)

FLASH-25517 - A blank page appears when clicking the Support link in the management GUI help menu. (S4)

FLASH-25374 - Manual data recovery should not require a manual change to restore cluster information. (S4)

FLASH-25558 - The 3D system view in the management GUI does not display correctly with some levels of the Chrome browser. (S5)

FLASH-25977 - Display logical capacity used in the user management GUI. (S5)

FLASH-25979 - All failed drives should no longer be powered off due to invalid temperature readings. (S5)

FLASH-25778 - SNMP output for port ID starts at 1 instead of 0. (S5)

FLASH-25797 - The CLI command `lssra` fails to execute on a canister that has been removed and reseated. (S5)

FLASH-25845 - While mapping volumes to a host using the GUI, a 'Loading' message should be presented rather than 'No items found.' (S5)

FLASH-25814 - A loading message on the GUI Dashboard should be center-aligned. (S5)

FLASH-25799 - Improve loading time for the GUI Dashboard. (S5)

FLASH-25387, 25385 - Improve wording for Service IP GUI panel. (S5)

FLASH-25386 - User name login for the GUI should not allow spaces. (S5)

FLASH-25375 - The 'Failed to connect to Key Server' event with ID 86008 and error code 1785 presents the 'Object Types' as 'UKNOWN'. (S5)

FLASH-25847 - The `lsenclosurecanister` CLI command reports a canister as offline when it is missing. (S5)

Return to top

Release 1.4.8.2

Release Date: January 31, 2019

The following issue was fixed in release 1.4.8.2:

FLASH-26321 - Repeated attempt to collect logs using the Service Assistant GUI may fail. (S5)

Release 1.4.8.1

Release Date: October 2. 2017

The following issue was fixed in release 1.4.8.1:

FLASH-27016 - Remediate vulnerability in system. (CVE-2018-1822). More information is available on this vulnerability through the following security bulletin: Security Bulletin: Vulnerability in the IBM FlashSystem models 840 and 900

Release 1.4.7.1

Release Date: September 12. 2017

The following issue was fixed in release 1.4.7.1:

FLASH-23256 - After upgrading to release 1.4.7.0, one of the Configuration Check Error (CCE) detection and handling engines on the flash module is not automatically started. (S3)

Release 1.4.7.0

Release Date: July 31. 2017

The following issues were fixed in release 1.4.7.0:

FLASH-22972, 23088, 23256, 23261, 22664, 23660, 24216, 22700 - (HIPER) Multiple enhancements made for Configuration Check Error (CCE) detection and handling. (S1)

FLASH-23211 - Staggered battery end of life is needed to ensure that both system batteries will not reach end of life simultaneously. (S1)

FLASH-22947 - Data sector check defeated by a corrupted field, which can lead to outages. (S2)

FLASH-22901 - Certify failures should not cause both RAID controllers to be failed repeatedly. (S2)

FLASH-22356 - Validation should be performed on rebuild/xverify to avoid out of bound addresses. (S2)

FLASH-22664 - Improve interface adapter failure recovery mechanism to prevent failing the RAID controller. (S2)

FLASH-22939 - On the unlikely occasion that system node canisters are placed into service state and rebooted, there may be a corrupt array and dual canister failures. (S2)

FLASH-24295 - iSCSI drops responses on SCSI reads when errors detected. (S3)

FLASH-22737 - Increase efficiency in low level data mapping to reduce I/O response times in certain pathological workloads. (S3)

FLASH-22938 - Array may move into the offline state after the active canister is removed and re-inserted into the enclosure. (S3)

FLASH-23267, 23269 - Allow local email users to turn warning email notifications off. (S3)

FLASH-23293 - Prevent canister lockup when Vital Product Data (VPD) is read during firmware upgrade. (S3)

FLASH-23316 - Shutting the system down with the stopsystem -force command could cause a warmstart if any flash modules are in the failed state or a RAID controller is in the service state. (S3)

FLASH-23484 - (HIPER) Prevent rare case of flash module sector errors causing a system outage. (S3)

Return to top

FLASH-23578 - Recovery backup only usable on the canister node that the command was issued from. (S3)

FLASH-23580 - Prevent timed out rebuild tasks from causing interfaces to be failed erroneously. (S3)

FLASH-23585 - Snap should reclaim space to prevent a canister disk from filling up. (S3)

FLASH-23722 - Service assistant commands hang sometimes after node failover. (S3)

FLASH-23894 - RAID controller failure could cause an assert. (S3)

FLASH-23978 - Battery reconditioning could start on one battery while the second battery is upgrading. (S3)

FLASH-23586 - The cluster recovery process is improved to handle systems with hardware updates needed. (S3)

FLASH-22463 - Stats reports inaccurate latency values. (S4)

FLASH-23589 - The informational event with ID 990138 is only generated the first time a VDisk is modified. (S4)

FLASH-23698 - The system properties window in the management GUI shows that encryption is not licensed when encryption is enabled. (S4)

Release 1.4.6.1

Release Date: April 13. 2017

The following issue was fixed in release 1.4.6.1:

FLASH-22861 - Remediate a vulnerability in Apache Struts Jakarta Multi-Part Parser Code Execution (CVE-2017-5638). More information is available on the IBM PSIRT Drive.

Release 1.4.6.0

Release Date: February 2, 2017

The following issues were fixed in release 1.4.6.0:

FLASH-12295 - Continuous and repeated loss of access of AC power on a PSU may, in rare cases, result in the report of a critical temperature fault. Using the provided cable secure mechanisms is highly recommended in preventing this issue. (S1)

FLASH-21880 - (HIPER) In rare cases, when both a rebuild read fails and a data reconstruction fails, a SCSI read should fail. (S1)

FLASH-21058 - Array goes offline due to an uncorrectable flash module failure. (S2)

FLASH-21782 - Cluster goes down due to a dead management PCIe link. (S2)

FLASH-15065 - Make use of the user installed certificate in REST API connections. (S3)

FLASH-17306 - An array with no spare did not report as degraded when a flash module was pulled. (S3)

FLASH-17724 - Adjusted InfiniBand (IB) ASIC timeouts to prevent erroneous system data stalls if the IB ASIC becomes unresponsive. (S3)

FLASH-20054 - Nodes have the potential to warm start after initializing. (S3)

FLASH-20869 - iSCSI VDisk mismatch from storage to host. (S3)

FLASH-21345 - FCoE interface adapters experience intermittent link-up issues. (S3)

FLASH-21528 - IB system may interpret connection as good after a firmware crash. (S3)

FLASH-21820 - 10Gb interface fails due to certify timeout. (S3)

FLASH-21857 - Internal error found after upgrade. (S3)

FLASH-21940 - The CLI allows the input of carriage return characters into certain fields after cluster creation resulting in invalid cluster VPD. (S3)

Return to top

FLASH-22005 - Internal error encountered after the enclosure hit an out of memory error. (S3)

FLASH-22143 - Improve stats performance to prevent SMNPwalk connection failure. (S3)

FLASH-18310 - RESTful API health check shows array as passing when all member drives are failed

FLASH-20258 - RESTful API health check reports formatting drives as online. (S4)

FLASH-21090 - The lsnodevpd command displays an incorrect FRU Number. (S4)

FLASH-21848 - Link to Knowledge Center from GUI DMP with error code 1802 is broken. (S4)

FLASH-21854 - GUI DMP with error code 2030 results in “Unable to proceed.” (S4)

FLASH-21920 - CLI and GUI don't get updated with the correct flash module firmware version after flash module FRU replacement. (S4)

FLASH-7931 - Include the system cluster name in Call Home heartbeats. (S4)

FLASH-21959 - Add a name field for an MDisk group in the return values of svcinfo lsmdiskgrp. (S5)

Release 1.4.5.0

Release Date: August 30, 2016

The following issues were fixed in release 1.4.5.0:

FLASH-18086 - Remediate vulnerabilities in OpenSSL (CVE-2016-0797, CVE-2016-0705, CVE-2016-2107)

FLASH-18362 - Remediate vulnerability in NSS (CVE-2016-1978).

FLASH-18799 - In iSCSI systems, nodes may go into a service state after a CCU which is preceded by a data recovery procedure. Fixing this issue also fixes iSCSI systems which were updating firmware for the FLASH-18373 issue. (S2)

FLASH-17560 - When a quorum device ID changes, previously raised events against this device cannot be marked as fixed, resulting in “A quorum device is not detected.” (S3)

FLASH-17791 - Multiple timeouts in iSCSI can cause a host to cease use of a target. (S3)

FLASH-17813 - CLI output for the “lsenclosurebattery” command erroneously reports that the replacement battery is online immediately after being installed. (S3)

FLASH-19407 - RESTful API background health checker statuses are not populated. (S3)

FLASH-19616 - The GUI notification engine hangs causing issues with DMPs. (S3)

FLASH-19886 - The GUI System page does not display offline battery info properly. (S4)

FLASH-19689 - SNMP daemon configuration doesn't support IPv6. (S4)

FLASH-19408 - A snap only collects SSD smartctl output from the configuration node. (S4)

FLASH-9798 - The CLI command “lsdrive drive_id” output does not reflect an updated “firmware_level” field after upgrade. (S5)

FLASH-16264 - The PSU DMP with error code 1298 and event ID 085007 shows that the event is not fixed when it is marked as fixed. (S5)

FLASH-19255 - CCU Stalled with internal errors. (S5)

Release 1.4.4.2

Release Date: June 28, 2016

The following issue was fixed in release 1.4.4.2:

Return to top

FLASH-18373 - An internal error may occur when host commands are used. This issue only exists in firmware versions 1.4.3.0 and later. The fix for this issue only applies to Fibre Channel systems. (S2)

Release 1.4.4.0

Release Date: May 27, 2016

The following issues were fixed in release 1.4.4.0:

FLASH-17998 - Internal error during error handling causes loss of access. (S1)

FLASH-17921, 16402 - Incorrect device discovery during Concurrent Code Upgrade (CCU) can cause access and data loss. (S1)

FLASH-17957, 15652 - After High Temp Shutdown of system, Array did not come back online. (S2)

FLASH-17500, 18051 - Internode communication issue causes CCU to stall. (S3)

FLASH-17821 - Internal error during CCU. (S3)

FLASH-17633 - Rare assert encountered. (S3)

FLASH-17812 - Battery failure Directed Maintenance Procedure (DMP) for error code 1114 indicates “Unable to proceed.” (S3)

FLASH-17856 - DMP for error 1114 for battery fault does not wait for a low charge battery FRU to charge. (S3)

FLASH-17859 - Battery “percent_charge” stays at old value if battery is removed or goes offline. (S3)

FLASH-17887, 15761 - Repeated CRC errors between interface and XBAR can fail a flash module. (S3)

Release 1.4.3.0

Release Date: April 28, 2016

The following issues were fixed in release 1.4.3.0:

FLASH-16313 - Authentication bypass using HTTP verb tampering is possible.

FLASH-15067 - Return code erroneously presents susceptibility to Cross-Site scripting.

FLASH-17149 - PSoC issues eventually lead to both canisters going into service state. (S1)

FLASH-17135 - Issues result when the same call home manager processes run simultaneously. (S1)

FLASH-17656 - Degraded components are included in the system thermal algorithm. (S1)

FLASH-17650 - Improve internal Flash checking to prevent access loss. (S1)

FLASH-17648 - Improve error handling of unresponsive flash chip. (S2)

FLASH-17732 - A canister node goes into service state 574 after a battery is degraded. (S2)

FLASH-17478 - Upgrade failed with the message “Unable to communicate with Systemmgr.” (S2)

FLASH-17448 - Fix iSCSI abort task for writes. (S2)

FLASH-16051 - Fix interface error reporting. (S2)

FLASH-17324 - Call home configuration cannot complete if network infrastructure is not ready. (S3)

Return to top

FLASH-17303 - Messages returned in response to issuing CLI commands 'svcinfo lsadminlun' and 'svcinfo lshostsubvolumemap' should be removed. (S3)
FLASH-16686 - During the error code 1039 Directed Maintenance Procedure (DMP), a failover popup erroneously appears before the DMP is complete. (S3)

FLASH-17528 - Double allocation of memory without the necessary free space leads to memory allocation failure. (S3)

FLASH-16010 – The ‘rmhost’ command on iSCSI hosts causes degraded nodes and T2 recovery. (S3)

FLASH-9266 - For RESTful API, ‘/system/time’ issues ‘setsystemtime’ with unusable context. (S3)

FLASH-6171 - Canister nodes should reboot in certain error conditions instead of requiring customer action. (S4)

FLASH-16471 - Add iSCSI connection diagnostic information. (S5)

FLASH-16265 - The field “Description” on the GUI easy setup has an inconsistent name on different panels. (S5)

FLASH-16005 - The filter search under Access User Groups in the GUI does not work well. (S5)

FLASH-15925 - In the User Properties menu, the OK button is enabled before any changes are made. (S5)

FLASH-15497 - The code level field and the test button on the GUI for the update utility are both grayed. (S5)

FLASH-16288 - Add a health check to RESTful API. (S5)

Release 1.4.0.10

Release Date: February 25, 2016

The following issues were fixed in release 1.4.0.10:

FLASH-15834 - Vulnerability in OpenSSL (CVE-2015-3194).

FLASH-15055 - Vulnerabilities in Network Security Services or NSS (CVE-2015-7181, CVE-2015-7182, and CVE-2015-7183).

FLASH-14599 - Vulnerability in Java™ (CVE-2015-4842). FLASH-15745 - Inquiry command after LUN reset incorrectly returned Unit Attention. (S2)

FLASH-15668 - The DMP with event ID 2030 “Internal error” indicates the wrong canister. (S2)

FLASH-15360 - Fault the Interface when FPGA buffer allocates or frees twice. (S2)

FLASH-15448 - Marking the event "Array mdisk is not protected by sufficient spares" as fixed should only fix the event in a system with three flash modules. (S2)

FLASH-15287 - A flashcard goes unresponsive when array certify is taking corrective action due to an error reporting issue. (S2)

FLASH-15975 - Update to allow upgrade to 1.4 from 1.3.0.4 and 1.2.1.8 releases. (S3)

FLASH-15866 - Node 574 error on reboot. (S3)

FLASH-15861 - A rare scenario finds sequential fail logic to be too aggressive. (S3)

FLASH-15488 - Both nodes assert during power up. (S3)

FLASH-15383 - The sector size column is missing in volumes grid of the GUI. (S3)

FLASH-15326 - Interface improvements necessary. (S3)

FLASH-15367, 15362 - Interface improvements necessary. (S3)

FLASH-15212 - iSCSI ExpCmdSN value exceeds the MaxCmdSN value. (S3)

FLASH-15254 - Improve signal margin on interface to/from RAID controller links. (S3)

FLASH-14930 - The DMP with the event ID 1061 (Event ID 085066) results in 'Unable to Proceed.' (S3)
FLASH-15668 - The DMP for error code 2030 displays the wrong canister information. (S4)

FLASH-15852 - Unexpected health check message seen in Service center. (S4)

Return to top

FLASH-15472 - The local file browse folder button does not work under Update System in the GUI. (S5)

FLASH-13202 - Logouts on iSCSI systems can cause a node failover in one scenario. (S5)

FLASH-10781 - VPD access does not quiesce system manager as expected. (S5)

Release 1.4.0.8

Release Date: December 22, 2015

The following issues were fixed in release 1.4.0.8:

FLASH-14869 - The telephone number field for notifications does not allow more than 10 digits to be entered. (S4)

FLASH-15329 - CLI help files were not translated in the 7.6.0.1 release. (S4)

Release 1.4.0.7

Release Date: December 8, 2015

The following issues were fixed in release 1.4.0.7:

FLASH-13706 - (HIPER) Potential undetected data corruption may occur due to a low probability race condition. The race condition has been observed on a system with a specific workload that is doing 1 to 2 GB/s of read operations with 250 MB/s of write operations. The write operations were less than 4K in size. (S1)

FLASH-13779 - Repeated interface panics causes an incorrect failure. (S2)

FLASH-12079 - A node timeout causes the Flash to fail. (S3)

FLASH-13052 - FC interface timeout issue results in a temporary error. (S3)

FLASH-13201 - Failed encryption validation causes a VM timeout. (S3)

FLASH-12463 - Flash failure due to Gateway to node CRC errors. (S3)

FLASH-11546 - Flash card failures are a result of an unexpected power off. (S3)

FLASH-13325 - Mitigate flashcard encryption error. (S3)

FLASH-13754 - The upgrade utility does not report a failed drive. (S4)

FLASH-14716 - Service manager panic experienced during upgrade. (S4)

FLASH-12906 - Stalled upgrade reports an upgrade failure error even after the upgrade completes successfully. (S4)

FLASH-14952 - Incomplete “chenclosurecanister” command can cause the nodes to assert. (S4)

FLASH-13654 - A node assert is experienced during upgrade. (S4)

FLASH-12839 - Export to CSV is not working on the performance page. (S4)

FLASH-13375 - RAID0 is no longer an option during easy setup through the GUI. (S5)

FLASH-13576 - A mandatory parameter is not included in the “ping” CLI help. (S5)

FLASH-13606 - Improve wording for restart and power off in the GUI menu for individual canister and entire system reboot or power off. (S5)

Release 1.3.0.9

Return to top

Release Date: January 8, 2018

The following issues were fixed in release 1.3.0.9:

FLASH-22859 - Remediate vulnerabilities in Java™ CPU (CVE-2016-5546, CVE-2016-5548, CVE-2016-5549, CVE-2016-5547, and CVE-2016-2183).

FLASH-23390 - Remediate a vulnerability in Apache Tomcat (CVE-2017-5647).

FLASH-25364 - Staggered battery end of life is needed to ensure that both system batteries will not reach end of life simultaneously. (S1)

FLASH-25519 - Validation should be performed on rebuild/xverify to avoid out of bound addresses. (S2)

FLASH-23501 - Shutting the system down with the stopsystem -force command could cause a warmstart if any flash modules are in the failed state or a RAID controller is in the service state. (S3)

Release 1.3.0.8

Release Date: April 13, 2017

The following issue was fixed in 1.3.0.8:

FLASH-22860 - Remediate a vulnerability in Apache Struts Jakarta Multi-Part Parser Code Execution (CVE-2017-5638). More information is available on the IBM PSIRT Blog.

Release 1.3.0.7

Release Date: February 28, 2017

The following issues were fixed in release 1.3.0.7:

FLASH-20584, 20733 - Remediate vulnerabilities in Apache Tomcat (CVE-2016-3092, CVE-2016-5387, CVE-2016-5388, CVE-2016-5385, CVE-2016-5386, CVE-2016-1000110, CVE-2016-1000105, and CVE-2016-1000111).

FLASH-20585 - Remediate vulnerabilities in Apache Struts (CVE-2016-4430, CVE-2016-4431, CVE-2016-4433, CVE-2016-4436, CVE-2016-4438, and CVE-2016-4465).

FLASH-20737 - Remediate vulnerabilities in OpenSSH (CVE-2015-5352, CVE-2015-6563, and CVE-2015-6564).

FLASH-22261 - Continuous and repeated loss of access of AC power on a PSU may, in rare cases, result in the report of a critical temperature fault. Using the provided cable secure mechanisms is highly recommended in preventing this issue. (S1)

FLASH-21881 - HIPER (Highly Pervasive): In rare cases, when both a rebuild read fails and a data reconstruction fails, a SCSI read should fail. (S1)

FLASH-21210 - Nodes have the potential to warm start after initializing. (S2)

FLASH-22264 - Cluster goes down due to a dead management PCIe link. (S2)

FLASH-21574 - The CLI allows the input of carriage return characters into certain fields after cluster creation resulting in invalid cluster VPD. (S3)

FLASH-22262 - Adjusted IB ASIC timeouts to prevent erroneous system data stalls if the IB ASIC becomes unresponsive. (S3)

FLASH-22328 - The DMP with error code 1114 for battery fault does not wait for a low charge battery FRU to charge. (S3)

FLASH-21975 - CLI and GUI don't get updated with the correct flash module firmware version after flash module replacement. (S4)

FLASH-22263 - The lsnodevpd command displays an incorrect FRU Number. (S4)

FLASH-22333 - The GUI system image does not always show USB drives installed when ports are active. (S4)

FLASH-22350 - Some text in some GUI fix procedures is not translated. (S4)

FLASH-20587 - The CLI command lsdrive drive_id output does not reflect an updated 'firmware_level' field after a system firmware upgrade. (S4)

Return to top

Release 1.3.0.6

Release Date: July 15, 2016

The following issues were fixed in release 1.3.0.6:

FLASH-16577 - Remediate vulnerabilities in Apache Tomcat (CVE-2015-5345, (CVE-2015-5346, CVE-2015-5351, CVE-2016-0706, CVE-2015-0714, CVE-2016-0763, (CVE-2015-5174).

FLASH-17238 - Remediate vulnerabilities in Apache Struts (CVE-2016-0785, CVE-2016-2162).

FLASH-17242, 18087 - Remediate vulnerabilities in OpenSSL (CVE-2016-0797, CVE-2016-0705, CVE-2016-2107).

FLASH-17956 - Remediate a vulnerability in NSS (CVE-2016-1978).

Remediate a vulnerability in Java (CVE-2016-0475).

FLASH-18049 - Improve internal Flash checking to prevent access loss. (S1)

FLASH-18132 - Issues result when the same call home manager processes run simultaneously. (S1)

FLASH-18134 - PSoC issues eventually lead to both canisters going into service state. (S1)

FLASH-18067 - Internal error handling causes loss of access. (S1)

FLASH-17914 - Degraded components are still used in the thermal algorithm. (S2)

FLASH-18053 - Upgrade failed with the message 'Unable to communicate with Systemmgr.' (S2)

FLASH-18062 - Fix interface error reporting. (S2)

FLASH-15900 - A rare scenario finds sequential fail logic to be too aggressive.(S3)

FLASH-17916 - Internode communication issue causes CCU to stall. (S3)

FLASH-19024 - Rare UTDE packet internal error causes warmstart and CCU stall. (S3)

FLASH-17011 - Missing internal system notification causes CCU to hang. (S3)

FLASH-18406 - Export to CSV does not work on the GUI performance page. (S4)

FLASH-16724 - Update system page reports the current software version is not supported. (S5)

Release 1.3.0.5

Release Date: March 1, 2016

The following issues were fixed in release 1.3.0.5:

FLASH-15905 - Marking 'Array Mdisk is not protected by sufficient spares' event as fixed should not work. (S3)

FLASH-14603 - Remediate a vulnerability in Java (CVE-2015-4872).

FLASH-15060 - Remediate multiple vulnerabilities related to Network Security services (NSS) (CVE-2015-7181, CVE-2015-7182, CVE-2015-7183).

FLASH-15835 - Remediate a vulnerability in OpenSSL (CVE-2015-3194).

FLASH-13795 - Remediate a vulnerability in Apache Struts (CVE-2015-5209).
FLASH-13574 - Remediate a vulnerability in cross-site request forgery (CSRF) (CVE-2015-7446).

Return to top

Release 1.3.0.4

Release Date: January 18, 2016

The following issues were fixed in release 1.3.0.4:

FLASH-14845, 14844 - Remediate vulnerability in PAM or Pluggable Authentication Module (CVE-2015-3238).

FLASH-13574 - Remediate Cross-Site Request Forgery or CSRF vulnerability.

FLASH-13535 - Remediate vulnerability in SSL/TLS.

FLASH-13369, 13368 - Remediate vulnerability in nss-softokn (CVE-2015-2730).

FLASH-13706 - HIPER (highly pervasive): Potential undetected data corruption may occur due to a low probability race condition. The race condition has been observed on a system with a specific workload that is doing 1 to 2 GB/s of read operations with 250 MB/s of write operations. The write operations were less than 4K in size. (S1)

FLASH-15207 - Repeated interface panics due to a bad interface cable can cause unnecessary component failures. (S2)

FLASH-14793 - A flash module can become unresponsive when array certify is running while hardware errors are being found. (S2)

FLASH-15489 - The nodes warmstart after being powered on due to an error in call home. (S3)

FLASH-13411 - Use of the command svcinfo lshostsubvolumemap causes the CLI to go down temporarily. (S3)

FLASH-13263 - VPD mismatch due to 8 Gb to 16 Gb conversion causes node asserts on upgrades to 1.3 firmware levels. (S3)

FLASH-15372 - Stalled upgrade reports an erroneous 'Failed to upgrade' error. (S3)

FLASH-15143 - The maximum number of host port objects decreases by one going from 1.2 to 1.3 code. (S3)

FLASH-14685 - Code upgrade stalls with internal error. (S3)

FLASH-12079 - Node timeout results in flash failure. (S3)

FLASH-12463 - Gateway to node CRC errors result in flash failure. (S3)

FLASH-11546 - Flash card failures occurred due to unexpected power off. (S3)

FLASH-13325 - Mitigation for flash module encryptor error. (S3)

FLASH-15254 - Improve signal integrity between canisters. (S3)

FLASH-15315 - The telephone number field length in the GUI does not match the requirements of SVC products. (S5)

FLASH-13484 - CLI help documentation for the ping command does not include new parameter. (S5)

Release 1.3.0.3

Release Date: October 6, 2015

The following issues were fixed in release 1.3.0.3:

FLASH-10534 - HIPER (highly pervasive): Potential undetected data corruption may occur when using Write Same commands. Direct attached FlashSystem 840 and 900 products can overwrite a buffer when Write Same commands are executing with heavy Input/Output usage. This is considered a highly pervasive problem involving firmware 1.2.x.x and 1.3.0.2. (S1)

FLASH-12982 - Issuing rmvdisk -force to remove a VDisk causes a node failover when host mappings exist. (S2)
FLASH-12837 - A node assert takes place when trying to add a node. (S2)

FLASH-12500 - Remediate vulnerabilities in Java (CVE-2015-2613, CVE-2015-2601, CVE-2015-2625, and CVE-2015-1931). (S2)

FLASH-11827 - When trying to install some packages, an 'Error in verifying the signature of the update package' message is produced. (S3)

Return to top

Release 1.3.0.2

Release Date: August 31, 2015

The following issues were fixed in release 1.3.0.2:

FLASH-10119, 13429 - HIPER (highly pervasive): Potential undetected data corruption may occur from interface error. FlashSystem 840 and 900 products can write inconsistent data to a host. This is considered a highly pervasive problem involving firmware versions 1.1.x.x and 1.2.x.x. (S1)

FLASH-11635 - Remediate vulnerabilities in OpenSSL (CVE-2015-1788, CVE-2015-1789, CVE-2015-1791, and CVE-2015-3216). (S1)

FLASH-12653 - Vulnerability in SSL/TLS discovered on REST API port (CVE-2015-2808). (S1)

FLASH-12537 - Canister is marked as 'failed' because it came online before completing the upgrade. (S2)

FLASH-11481 - The node throws an assertion exception for exceeded temperature on an unused drive. (S2)

FLASH-11958 - Stats can fill the /dumps folder to capacity, which disables the node from booting. (S2)

FLASH-12689 - An unexpected canister powering off can, in some cases, cause loss of access to data due to interface failure. (S2)

FLASH-12492 - Not able to rekey if encryption was enabled after the initial array creation and a node failover has occurred on firmware version 1.1.3.x or 1.2.x.x. (S2)

FLASH-12271 - The RAID controller was falsely marked as 'failed' instead of a flash module in a particular double flash module failure scenario. (S2)

FLASH-12219 - An unexpected canister powering off can cause the other canister to warm start. (S2)

FLASH-12061 - The controller panics when no type is set on an unresponsive interface. (S2)

FLASH-9320 - Simultaneous double flash fails can result in the incorrect component being marked as 'failed.' (S2)

FLASH-11595 - Interface incorrectly fails during a sequential double flash module failure scenario. (S2)

FLASH-11567 - Spikes in Input/output latency occur due to encryption validation. (S3)

FLASH-12387 - GUI incorrectly uses the '-force' option to reboot or power off a canister or system. (S3)

FLASH-12331 - iSCSI Check Condition sense data is invalid. (S3)

FLASH-12299 - iSCSI 'Desired Data Length' incorrectly exceeds 'MaxBurstLength.' (S3)

FLASH-12298 - iSCSI packet with garbled parameters incorrectly causes port to go offline. (S3)

FLASH-12296 - iSCSI duplicate 'InitiatorName' key is not rejected at login as it should be. (S3)

FLASH-12236 - iSCSI target does not discard command with invalid CmdSN. (S3)

FLASH-10687 - Archive stats are wrong after a canister power off. (S3)

FLASH-10170 - 'Abort Task Set' incorrectly compares sequence numbers. (S3)

FLASH-12237, FLASH-11964, FLASH-11962, FLASH-11943 - iSCSI improvements made for path failures. (S3)

FLASH-12175 - Incorrect memory free error for canceled UNMAP commands. (S3)

FLASH-12174 - Interface does not UNMAP data in a particular scenario. (S3)

FLASH-12173 - Interface allows host to surpass the UNMAP limit on block descriptors. (S3)

FLASH-11944, FLASH-11943 - High traffic on FC and iSCSI systems can cause a single command to stall. (S3)

FLASH-11933 - Traffic on iSCSI can stall if something is put in a queue. (S3)

FLASH-10276 - Improvements needed for link speed for iSCSI. (S3)

Return to top

FLASH-12227 - Unexpected event for drive failure and replacement should actually be a quorum error. (S3)

FLASH-11468 - GUI shows canister offline while CLI shows canisters online. (S3)

FLASH-11184 - 'Neighbor table overflow' spamming causes Ethernet connectivity issues. (S3)

FLASH-12283 - Stale interface logins are not removed on failure as expected. (S3)

FLASH-11337 - Fault LED comes on after drive replacement and the resetleds command is issued.

FLASH-11051 - GUI becomes unresponsive. (S3)

FLASH-10111 - A link error between the drive and RAID controller gets incorrectly propagated and incorrectly fails the RAID controller. (S3)

FLASH-11477 - Flash module reports the incorrect temperature on node timeout, which results in a false critical temperature failure. (S3)

FLASH-11874 - A quick canister reseat can lead to the canister reporting 'degraded.' (S4)

FLASH-11359 - A nonconcurrent upgrade fails due to an issue in the full system boot upgrade. (S4)

FLASH-9930 - The GUI should allow the user to cancel if upgrade is in 'prepared' state. (S4)

FLASH-9241 - The GUI does not report the correct output for the lsupdate command. (S4)

FLASH-10516 - Improve logging. (S4)

FLASH-9152 - The status LED is incorrectly lit when canister is off. (S4)

FLASH-12393 - Some system stats incorrectly continue to update. (S4)

FLASH-10157 - Improve management controller packet handling. (S4)

FLASH-6114 - The svcinfo lsnode CLI command incorrectly displays different port information than the lsportfc command. (S4)

FLASH-5869 - The 'fc_io_port_WWPN' field of the sainfo lsservicestatus command is inconsistent between protocols. (S4)

FLASH-4288 - The 'node_code_build' field of the sainfolsservicestatus command does not display the complete build number. (S4)

FLASH-9962 - Issuing lsdumps -prefix with an invalid directory causes a node failover. (S4)

FLASH-10377 - Make battery output improvements. (S5)

FLASH-12047 - Improve system manufacturing tests. (S5)

FLASH-10034 - Improve system logs. (S5)

FLASH-12392 - GUI snaps are missing files from the 'cimom' directory. (S5)

Upgrading firmware

Use the following sections to perform firmware upgrades for your systems to the current release.

Warning: Please read all the instructions below before upgrading.

Release overview

If you are upgrading to this release and your system is healthy, you can perform a Concurrent Code Upgrade (CCU). A CCU is a non-disruptive upgrade and is the preferred upgrade method. For general instructions on performing upgrades, refer to the FlashSystem Knowledge Center.

Return to top

Supported upgrade paths

The following upgrade paths are supported for this release. Note that customers with AE3 hardware have fewer supported upgrade paths than customers with AE2 hardware.

Note: Support for AE2 hardware in 1.5.x releases starts in firmware version 1.5.1.0.

AE2				**AE3**	
From	**From/To**	**From/To**	**To**	**From**	**To**
1.2.0.x	--> 1.2.1.10	--> 1.5.x	--> 1.6.1.2	1.5.0.0	--> 1.6.1.5
1.2.1.x	--> 1.5.x	--> 1.6.1.2		1.5.1.x	--> 1.6.1.5
1.3.0.x	--> 1.5.x	--> 1.6.1.5		1.5.2.x	--> 1.6.1.5
1.4.0.x	--> 1.5.x	--> 1.6.1.5		1.6.0.x	--> 1.6.1.5
1.4.3.0	--> 1.5.x	--> 1.6.1.5		1.6.1.x	--> 1.6.1.5
1.4.4.x	--> 1.5.x	--> 1.6.1.5			
1.4.5.0	--> 1.5.x	--> 1.6.1.5			
1.4.6.x	--> 1.5.x	--> 1.6.1.5			
1.4.7.x	--> 1.5.x	--> 1.6.1.5			
1.4.8.x	--> 1.5.x	--> 1.6.1.5			
1.5.1.x	--> 1.6.1.5				
1.5.2.x	--> 1.6.1.5				
1.6.0.x	--> 1.6.1.5				
1.6.1.x	--> 1.6.1.5				

Preparing to upgrade

CCU is a non-disruptive upgrade, which means that the system remains online throughout the process and that you can continue to access data normally. As a precaution, it is recommended that the upgrade occur during a time of reduced traffic. During the upgrade, the interface adapters in each canister are taken offline temporarily to be upgraded. This might impact performance or throughput. The impact is more noticeable under heavy load conditions. With a properly configured multi-path configuration, access to your data is always maintained.

To ensure a successful, non-disruptive upgrade, you should verify that your interface ports are all online and all the system hardware is functioning normally. Ideally, you should have the following:

- All host interfaces should be online. An active multi-path configuration is required to ensure no loss of access during the upgrade.
- If you have enabled automatic battery reconditioning, it should be disabled a day in advance and re-enabled after the upgrade is completed so that battery reconditioning does not interfere with the planned upgrade.
- Both batteries should be online and charged. Use the CLI command `lsenclosurebattery` or the management GUI under **Monitoring** --> **Systems** to verify battery status. Note: If the battery status is 'reconditioning,' the firmware upgrade will not be allowed to start until after reconditioning completes. If the battery status is 'reconditioning required,' then you may proceed with the upgrade and perform reconditioning on the battery later. Note also that battery reconditioning can take up to 24 hours to complete.
- All hardware should be online and functioning normally. There should be no unfixed alerts in the event log (see the exceptions below).

Running the ugprade test utility is a required step before concurrent upgrade in firmware versions after 1.2.0.11. The utility checks for problems in the system that might prevent the upgrade from completing successfully and either warns the user or blocks the user from proceeding. IBM Support recommends that all users planning to upgrade run the utility a full day in advance so that any issues called out by the utility can be remedied without delaying the planned upgrade.

To view checks that the upgrade utility makes before an upgrade, see the the release notes for the latest upgrade test utility posted along with each available firmware package on IBM Fix Central.

Important: Before you begin the upgrade, we recommend that you perform a backup of your data and a backup of the FlashSystem configuration. To back up the configuration, log into the cluster management IP address and issue the following command using admin-level authority:

```
svcconfig backup
```

Return to top

Optionally, you can copy the configuration backup file from the FlashSystem to your workstation using secure copy (scp) on Linux or PuTTY secure copy (pscp.exe) on Windows as in the following examples:

(Using Linux)

```
scp superuser@cluster_ip:/dumps/svc.config.backup.* .
```

(Using Windows)

```
pscp -unsafe superuser@cluster_ip:/dumps/svc.config.backup.* .
```

Note: Do not ignore the periods shown above at the end of each command. In addition, replacement of italicized descriptions within angle brackets with appropriate information is required.

Posted along with the release notes and upgrade files on Fix Central are md5sum text files. These files exist for each update file so that the user can verify that the update file was downloaded correctly.

Performing the upgrade

It is highly recommended that the upgrade be performed using the web-based cluster management interface known as the management GUI. Instructions are available for performing a CCU in IBM Knowledge Center. Search for 'IBM FlashSystem 900,' then navigate to Upgrading the system. Included is information on retrieving software packages, using the update test utility, and automatically updating using either the GUI or the CLI.

Troubleshooting

Use the following sections to troubleshoot problems that may occur during the upgrade process.

Stalled upgrade

If the upgrade takes more than two hours to complete, it may have stalled. Upgrade status is viewed by issuing lsupdate CLI command or by going to **Settings** --> **System** --> **Update System** in the GUI. Both show a 'Stalled' status. In most cases, this can be resolved by aborting the upgrade and reattempting the upgrade after the system downgrades to its original level. To abort the upgrade, issue the `applysoftware -abort` CLI command or click the 'Stop Upgrade' button in the GUI.

After the system is downgraded, you can reattempt your upgrade from the GUI or CLI. If the upgrade stalls repeatedly or if you have alerts which cannot be cleared, contact IBM Support.

Failures during upgrade

You may get a battery or quorum alert during upgrade due to required reconfiguration. These alerts should be automatically cleared when the upgrade is completed. They may be visible from the Events view of the management GUI if the filter is set to 'Show All,' but they should no longer appear in the Recommended Actions, Unfixed Messages, or Alerts views. If you see unfixed battery or quorum alerts after an upgrade is complete, contact IBM Support.

If the upgrade has failed or stopped due to a hardware failure, you will see the 'Hardware Failed' status.

If you suspect a hardware failure, issue the `lsupdate` command to confirm the state of your system. This command shows that the system is in a `hardware_failed` state and the event log contains a 'System upgrade suspended' event. You may resume the upgrade by issuing the `applysoftware -resume -force` command for the following conditions:

- PSU unsupported events
- Battery fault type 1 events that are fixed and online according to the CLI command `lsenclosurebattery`
- Fan events

If the upgrade cannot be resumed or you have other alerts which cannot be cleared, contact IBM Support. The battery reconditioning feature calibrates the gauge that reports the amount of charge on the batteries. On systems that have been installed for 10 months or more or systems that have experienced several power outages, the recommendation to run 'battery reconditioning' will appear in the event log shortly after upgrading. This is normal. Use the management GUI to run a DMP for this error or see the FlashSystem Knowledge Center to view how to properly issue the `chenclosureslot` command in reference to this issue. Use the following link to access the IBM Documentation page for battery reconditioning.

Return to top

Contact information

Call IBM at 1-800-IBM-SERV (1-800-426-7378). To find contact information for a specific region, visit the IBM directory of worldwide contacts.

Revision history

The following information reflects changes made to this document.

Revision number	Description	Date
1.0	Original version.	October 31, 2022

Copyright notice