

IBM FlashSystem[®] V9000

Firmware Version 1.5.2.10

Release Date: October 20, 2021

Applicable systems

This release is only supported for the IBM FlashSystem V9000 storage enclosure, Machine Types and Models (MTM) 9846-AE3 and 9848-AE3.

Product resources

IBM FlashSystem V9000 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 V9000 or visit the [IBM Redbooks[®]](#) website for the IBM FlashSystem V9000 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 Program Temporary Fix (PTF) for IBM FlashSystem V9000 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

There are no fixes in this release outside of those described in under "Remediated security vulnerabilities" below. To view fixes from earlier releases, see the [Release history](#). Available firmware releases are listed on [IBM Fix Central](#). For issue severity definitions, see the [Bug severity legend](#).

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](#)

Return to top

Remediated security vulnerabilities

The following security vulnerability has been remediated in this release:

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 features

The following information lists the features that come with the 1.5 release of IBM FlashSystem V9000 product.

- 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.
- 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.

Known issues

Please be aware of the following known issue:

- 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 1.5.2.4, 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)

Release history

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

— Release 1.5.2.9

Release Date: May 3, 2021

Return to top

The following issues were fixed in release 1.5.2.9:

FLASH-29779 - Add data integrity protection between the PCIe link to the HBA and the DDR memory. (S1)

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 1.5.2.8

Release Date: January 2, 2021

The following issues were fixed in release 1.5.2.8:

FLASH-29746 - Add additional logic to protect against rare transient error cases that cause data loss. (S1)

A vulnerability in OpenSLP ([CVE-2019-5544](#)) has been remediated in this release. For more information on this vulnerability, see IBM's security bulletin: [Security Bulletin: OpenSLP vulnerability affects IBM SAN Volume Controller, IBM Storwize, IBM Spectrum Virtualize and IBM FlashSystem products](#)

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 \(CVE-2020-13935\)](#).

– Release 1.5.2.7

Release Date: April 6, 2020

The following issues were fixed in release 1.5.2.7:

FLASH-29407 - HIPER (Highly Pervasive): A node warm start is possible after a flash module fails, which could result in a node failover. (S1)

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

FLASH-29475 - A mitigation was added for the interface controllers to prevent system outages due to internal hardware failure. (S1)

FLASH-29639 - An "invalid" health reading should not fail a flash module. (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-28177 - The event with ID 988011 and description "Array storage is low on available space" should be able to be manually marked as fixed. (S5)

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 1.5.2.6

Release Date: October 7, 2019

The following issues were fixed in release 1.5.2.6:

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

FLASH-28505 - A flash module communication error could sometimes cause a loss of access due to a rare timing condition. (S2)

FLASH-29154 - Changing the default security protocol to 4 without a preexisting array could block array creation. (S5)

FLASH-28787 - Remediate a vulnerability in Java which affects IBM FlashSystem V9000 ([CVE-2019-2602](#)).

Return to top

FLASH-29146 - Remediate multiple vulnerabilities in the Linux kernel which affect IBM FlashSystem V9000 ([CVE-2019-11479](#), [CVE-2019-11478](#), and [CVE-2019-11477](#)).

More information is available on these vulnerabilities through the following security bulletins:

- [Security Bulletin: A vulnerability in Java affects IBM FlashSystem V840 and V9000](#)
- [Security Bulletin: Multiple Vulnerabilities in the Linux kernel affect the IBM FlashSystem models V840 and V9000](#)

– 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)

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)

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-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-26913 - 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.

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](#)).

FLASH-28611, 27717, 26996, 26556 - Remediate multiple vulnerabilities in Java which affect IBM FlashSystem V9000 ([CVE-2018-12547](#), [CVE-2018-2180](#), [CVE-2018-1517](#), and [CVE-2018-2783](#)).

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 V9000 ([CVE-2018-11784](#)).

FLASH-27632 - Remediate a vulnerability in OpenSLP which affects IBM FlashSystem V9000 ([CVE-2017-17833](#)).

FLASH-28244 - Remediate a vulnerability in HTTP which affects IBM FlashSystem V9000.

More information is available on listed vulnerabilities through the following security bulletin:

- [Security Bulletin: A vulnerability affects the IBM FlashSystem 840 and 900](#)
- [Security Bulletin: Multiple Vulnerabilities in Java affect IBM FlashSystem V840 and V9000](#)
- [Security Bulletin: Multiple Vulnerabilities in the Linux kernel affect IBM FlashSystem V840 and V9000](#)
- [Security Bulletin: A vulnerability in OpenSLP affects IBM FlashSystem V840 and V9000](#)
- [Security Bulletin: A vulnerability in Apache Tomcat affects IBM FlashSystem V840 and V9000](#)

– Release 1.5.2.1

Return to top

Release Date: October 15, 2018

The following issues were fixed in release 1.5.2.1:

FLASH-26929 - Remediate a vulnerability in Apache Struts which affects IBM FlashSystem 900 ([CVE-2018-11776](#)). More information is available on this vulnerability through the following security bulletin: [Security Bulletin: A vulnerability in Apache Struts affects the IBM FlashSystem 840 and 900](#)

FLASH-26705 - AE3 flash modules may erroneously present to be in low health. (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)

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

FLASH-26424 - Improved RAID error handling for unresponsive flash modules to prevent rare data error. (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 V9000 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 issues were fixed in release 1.5.1.0:

[Return to top](#)

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

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

FLASH-25562 - Users with 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. (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-25772 - In rare cases, a PSU fan can become stuck at high speed unnecessarily. (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, 35385 - 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 'UNKNOWN'. (S5)

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

[Return to top](#)

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](#).

Supported upgrade paths

The following upgrade paths are supported for this release.

From	To
1.5.0.x	--> 1.5.2.10
1.5.1.x	--> 1.5.2.10
1.5.2.x	--> 1.5.2.10

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.
- 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 unfix alerts in the event log (see the exceptions below).

Running the upgrade 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
```

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.

[Return to top](#)

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 V9000,' 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 `lupdate` 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 `lupdate` 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:

- o PSU unsupported events
- o Battery fault type 1 events that are fixed and online according to the CLI command `lenclosurebattery`
- o 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.

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 20, 2021

Copyright notice

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of IBM Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol, indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available [here](#).

The following terms are trademarks of other companies:

- Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
- Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other product and service names might be trademarks of IBM or other companies.