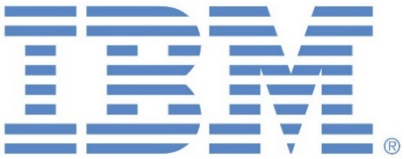

IBM FlashSystem 720 and IBM FlashSystem 820

Firmware Version 6.3.2, patch 7

Release Notes

August 28, 2017

Contents

1.0 Applicable systems

This release is recommended for the following systems:

- IBM FlashSystem® 720, machine type 9831
- IBM FlashSystem 820, machine type 9831
- IBM RamSan® 720, machine type 9834
- IBM RamSan 820, machine type 9834

2.0 Bug severity legend

The following explains the bug severity ranking used in Section 4.1 for key fixes and in Section 7.0, the release history:

S1: Highest	Recommend upgrade for all users as soon as possible.
S2: Medium	Recommend upgrade for all users at the next scheduled maintenance window.
S3: Average	Recommend upgrade at the next scheduled maintenance window for users experiencing these issues. All other users may wish to upgrade at the next scheduled maintenance window.
S4: Low	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: Lowest	Upgrade is not necessary. This would include a mostly cosmetic or minor annoyance fix.

3.0 Release summary

These release notes are specifically written to identify and describe security vulnerabilities remediated by patch 7 of release 6.3.2. Release 6.3.2 is also recommended for systems where customers are using the GUI for system event log generation and for AIX environments. Vulnerabilities in multiple services have been remediated. Each of these items are described below. See Section 4.1 for more information on the specific vulnerabilities remediated in the current release.

- **Network Time Protocol (NTP)** provides time synchronization between systems.
- **Libxml2** is a code library used to parse Extensible Markup Language (XML).
- **OpenSSH** is a tool which provides remote connection using Secure Shell (SSH).
- **BusyBox** provides multiple tools in a single executable file.
- **OpenLDAP** is open source and provides Lightweight Directory Access Protocol (LDAP) for free.
- **Python** is a programming language.
- **OpenSSL** is a toolkit that implements the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols, as well as a full-strength, general purpose cryptography library.
- **Network Security Services (NSS)** is a set of libraries designed to support cross-platform development of security-enabled client and server applications.
- **GNU C Library**, also called glibc, is a popular implementation of the C standard library for the C programming language.
- **Bash** is a widely-used command line language and Unix shell.
- **Core Utils** is a package of commonly used command line utilities.
- **Curl** is a programming language.

4.0 Latest changes

This release is a Program Temporary Fix (PTF) which remediates several security vulnerabilities.

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.

http://www.ibm.com/support/fixcentral

4.1 Key trackers

The following fixes are included in this patch for release 6.3.2. See the release history in Section 7.0 for other fixes in this and previous releases. Release 6.3.2, patch 7 includes the following security remediations:

Note: All issues fixed in this release are relevant to security vulnerabilities. Use the Common Vulnerabilities and Exposures (CVE) identifiers provided below to find more information on each vulnerability by searching the CVE website: https://cve.mitre.org/cve/cve.html

Descriptions of each affected item are given in Section 3.0. Severity levels are not used for security issues.

- Vulnerabilities in NTP (CVE-2015-5194, CVE-2015-5195, CVE-2015-5219, CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-2015-7702, CVE-2015-7703, CVE-2015-7852, CVE-2015-7977, CVE-2015-7978, CVE-2015-7979, CVE-2016-1547, CVE-2016-1548, CVE-2016-1550, CVE-2016-2518, CVE-2016-7426, CVE-2016-7429, CVE-2016-7433, CVE-2016-9310, and CVE-2016-9311).
- Vulnerabilities in libxml2 (CVE-2016-1762, CVE-2016-1833, CVE-2016-1834, CVE-2016-1835, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, CVE-2016-1840, CVE-2016-3627, CVE-2016-3705, CVE-2016-4447, CVE-2016-4448, and CVE-2016-4449).
- Vulnerabilities in OpenSSH (CVE-2015-5352, CVE-2015-6563, CVE-2015-6564, and CVE-2015-8325).
- Vulnerabilities in BusyBox (CVE-2014-4607 and CVE-2014-9645).
- A vulnerability in OpenLDAP (CVE-2015-6908).
- Vulnerabilities in Python (CVE-2016-0772, CVE-2016-5699, and CVE-2016-1000110).
- Vulnerabilities in OpenSSL (CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-2183, CVE-2016-6302, CVE-2016-6304, CVE-2016-6306, CVE-2016-8610, and CVE-2017-3731).
- Vulnerabilities in NSS (CVE-2016-2834, CVE-2016-5285, CVE-2016-8635, CVE-2017-5461, and CVE-2017-7502).
- Vulnerabilities in GNU C Library (CVE-2014-9761, CVE-2015-8776, CVE-2015-8778, CVE-2015-8779, and CVE-2017-1000366).
- Vulnerabilities in bash (CVE-2016-0634, CVE-2016-7543, and CVE-2016-9401).
- A vulnerability in core utils (CVE-2017-2616).
- A vulnerability in curl (CVE-2017-528).

4.2 Currently supported specifications

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 Protocol for SCSI - v3
SCSI-SRP	SCSI RDMA Protocol - v1
FC-PH-3	Fibre Channel Physical and Signaling Interface - v3
FC-AL-2	Fibre Channel Arbitrated Loop - v2
IBTA-1.2	InfiniBand Trade Association Architecture Specification - v1.2

5.0 Upgrading firmware

Warning: Failure to involve technical support after encountering upgrade problems may lead to a loss of data and system instability. See Section 8.0 for Technical Support contact information.

Use the following instructions to upgrade to the latest firmware level:

1. Verify the current firmware level and system type. 6.x.x firmware is valid for all FlashSystem 720 and FlashSystem 820 systems.
2. Backup the contents of the storage system to an external device. This is a standard safety precaution to prevent accidental data loss.
3. Backup system configuration information.
4. Ensure that a copy of the firmware that is currently installed is available. The latest firmware is available on Fix Central. For older firmware levels, contact IBM Support.
5. Stop all network traffic to the system.
6. Perform a clean re-boot of the system.
7. Upload the patch using either the web interface or the Windows command-line executable.
8. To upload the patch using the web interface, use one of the following methods:
    a. Point a browser at the unit IP address or hostname.
        i. Log in using admin group level permissions or higher. You must uncheck the “Secure Connection (SSL)” check box in order to login and upload the patch. See the figure below for reference.

            Note: Unchecking the SSL check box in order to log in through the GUI is only applicable to patch 5 and is a temporary workaround.

Figure 1.Logging into the system.

        ii. Expand the system tree node in the left window pane.
        iii. Right-click on the management node and select **Firmware Update**.
        iv. Follow the wizard instructions to locate the patch file, which has the following naming format: FlashSystemXXX-v6_X_X.patch
    b. To upload the patch using the Windows command-line interface (CLI):

i. Locate the `uploadPatch.exe` executable program included in the firmware package. If the firmware package does not include the program, contact Technical Support to obtain it.
ii. Execute the patching program, giving it the patch file name and the IP address or hostname of the unit, as seen below:

```
uploadPatch.exe patchfilename network_address_of_system
```

The patch filename has the following format: `FlashSystemXXX-v6_X_X.patch`

c. To upload the patch using the Linux CLI:
i. Locate the `uploadPatch` or `uploadPatch_x64` (for 64-bit Linux distributions) executable program included in the firmware package. If the firmware package does not include the program, contact Technical Support to obtain it.
ii. Execute the patching program, giving it the patch file name and the IP address or hostname of the unit, as shown below:

```
uploadPatch patchfilename network_address_of_system
```

The patch filename has the following format: `FlashSystemXXX-v6_X_X.patch`

9. The patch may take several minutes to upload. After the patch upload is complete, you are presented with the status of the upload.

Note: If there are any errors or the upload does not complete after at least 5 minutes, contact Technical Support before proceeding. An uploaded firmware patch can be canceled before the system is restarted. To cancel a patch, click **Cancel Patch** and confirm that you do not want to apply the currently patch that is currently uploaded.

10. Once you have successfully uploaded the patch to the system, the system must be rebooted for the changes to take effect. To do this, use one of the following methods:
    - From the web interface, click the system IP address in the system tree to display the system panel, then click Restart or Shutdown to reboot the system and begin the patch process.
    - From the CLI, run the following command: `system reboot`

Note: Do not reboot if you notice any error messages. Contact Technical Support if anything looks unusual after applying the patch file.

11. The reboot command may disconnect your CLI session. Reconnect the system and run the command `log follow` or monitor the progress in the Recent Event Log window on the lower half of the GUI screen. The patch process requires from 30 to 60 minutes to complete. Once complete, the message "Successfully applied all patch images" appears.

Attention: If the patch process is interrupted by power loss, the system can become unusable. If your system's patch is interrupted or stalls for longer than one hour, immediately contact Support. Do not disconnect the power cords or take any other action to resolve the situation unless recommended by Support.

12. After rebooting the system, the system boots with the new firmware level and all previous settings are maintained.
13. Close and re-open all browser windows which have the web interface connected to the system to ensure that any firmware changes to the web interface are re-downloaded to the browser.
14. In the unlikely event of a patch failure or a failure of the unit to successfully complete the power-cycle, immediately contact Technical Support before attempting to diagnose the problem.

6.0 Known issues and workarounds

The following describes current known issues and the workarounds for these issues that you should be aware of:

- 19605 - The Qlogic SANbox2-8c 2Gb switch is not supported in Arbitrated Loop topologies.
- 18088 - When direct-connected to an Emulex HBA in Arbitrated Loop topology, "Unhandled ELS request" events may be emitted to the FlashSystem event log during loop initialization. These messages are harmless and can be safely ignored.
- The 6.X.X firmware web management tool is incompatible with the 3.X.X firmware web management tool. Please close and re-open all web browser windows when switching between systems with different versions.
- Due to a Java bug (Bug ID 6183877), occasionally typed text will not be displayed in text fields in the web management application. This only occurs with Linux. The workaround is to click off of the window containing the text field and then back on the text field itself.

7.0 Release history

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

Release 6.3.2, patch 6

The following vulnerabilities were remediated in version 6.3.2, patch 6:

- Vulnerabilities in OpenSSL have been remediated (CVE-2016-2108, CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-0799, CVE-2016-2842, CVE-2016-2109, CVE-2015-3197, CVE-2016-0702, CVE-2016-0705, CVE-2016-0797, and CVE-2016-0800).
- Vulnerabilities in NSS have been remediated (CVE-2016-1978, CVE-2016-1979, and CVE-2016-1950).
- Vulnerabilities in Kerberos have been remediated (CVE-2015-8629 and CVE-2015-8631).

Release 6.3.2, patch 5

The following issue was fixed in version 6.3.2, patch 5:
RSF-3329 - The server SSL certificate signing algorithm has been updated per new security standards in Java™ 7. This update fixes browsers that fail login with the error "java.security.cert.CertificateException: Certificates does not conform to algorithm constraints." For a temporary workaround, deselect the box to use SSL in the Web Monitor application and then login and update the firmware. (S4)

Release 6.3.2, patch 4

The following security vulnerabilities were fixed in version 6.3.2, patch 4:

Note: All issues fixed in this release are relevant to security vulnerabilities. Use the CVE numbers provided to find more information on each vulnerability.

- Vulnerabilities in freetype has been remediated (CVE-2014-9657, CVE-2014-9658, CVE-2014-9660, CVE-2014-9661, CVE-2014-9663, CVE-2014-9664, CVE-2014-9667, CVE-2014-9669, CVE-2014-9670, CVE-2014-9671, CVE-2014-9673, and CVE-2014-9674).
- Vulnerabilities in krb5 have been remediated (CVE-2014-5352, CVE-2014-5353, CVE-2014-5355, CVE-2014-9421, and CVE-2014-9422).
- Vulnerabilities in NTP have been remediated (CVE-2014-9297, CVE-2014-9298, CVE-2015-1798, CVE-2015-1799, and CVE-2015-3405).
- Vulnerabilities in glibc have been remediated (CVE-2014-8121, CVE-2013-7424, CVE-2013-7423, and CVE-2015-1781).
- A vulnerability in Net-SNMP has been remediated (CVE-2015-5621 and CVE-2014-3565).
- A vulnerability in nss-softokn has been remediated (CVE-2015-2730).
- A vulnerability in lighttpd has been remediated (CVE-2015-3200).
- A vulnerability in openSSH has been remediated (CVE-2015-5600).
- Vulnerabilities in OpenSSL have been remediated (CVE-2014-8176, CVE-2015-1789, CVE-2015-1790, CVE-2015-1791, CVE-2015-1792, and CVE-2015-3216).
- Vulnerabilities in curl have been remediated (CVE-2014-3613, CVE-2014-3707, CVE-2014-8150, CVE-2015-3143, and CVE-2015-3148).
- A vulnerability in libxml2 has been remediated (CVE-2015-1819).
- A vulnerability in pam has been remediated (CVE-2015-3238).
- Vulnerabilities in NSS have been remediated (CVE-2015-7181 CVE-2015-7182 CVE-2015-7183).

Release 6.3.2, patch 3

The following issues were fixed in version 6.3.2, patch 3:

33295 - Remediate security vulnerabilities for SSL/TLS. (S2)
33297 - Remediate security vulnerabilities for OpenSSL. (S2)

Release 6.3.2, patch 2

The following issues were fixed in release 6.3.2, patch 2:
33277 - Single interface DMA timeouts after 248 days results in a failure that could result in failing multiple flashcards. (S1)
33257 - Failing management control could result in bringing the storage offline if there were previous flashcard replacements since the last power cycle. (S2)

Release 6.3.2, patch 1

The following issue was fixed in release 6.3.2, patch 1:
32713 - In 6.3.2, the system event log web application was not functioning. (S3)

Release 6.3.2

The following issues were fixed in version 6.3.2:
29078 - Flashcards now support FPGA configuration checks and correction.
32241 - The built-in read sweeper for the flashcard would skip some data pages. This means that over time, data not read by the application could eventually result in uncorrectable data errors. (S1)
29018 - A single over-voltage battery will no longer cause the system to shut down. (S2)
29073 - Prevent systems from having intermittent CRC errors from the RAID controller to the flashcards. Only flashcard-1 and flashcard-12 were exposed to this issue. (S2)
30379 - If the flashcard encounters an uncorrectable error from non-host data reads, it will set the health state to warn. (S2)
31163 - Some flashcards receive an internal error that would cause the flashcard to fail. The firmware has been modified to prevent these issues. (S2)
30225 - A system message will now be displayed if the active controller is no longer syncing configuration changes to the other management controller. (S3)
32042 - An Ethernet packet storm could cause the system to shut down. (S3)
24914 - Prevent system reboots from occurring while patching is in progress. (S3)
25377 - An uninitialized flashcard can now be formatted as a spare. (S3)
25590 - A slow memory leak in the SNMP server could cause the system to run out of memory if SNMP clients were frequently requesting information. (S3)
28406 - Removed support for weak encryption methods via SSL to the FlashSystem. (S3)
28493 - After executing the "lu access add group" command, the system would not send any more call home events until the next system reboot. (S3)
29164 - All system messages will now generate call home events when they are added or removed. (S3)
30521 - Deleting LDAP users is now properly prevented from occurring. And attempting to do such will not create duplicate user entries. (S3)
31069 - Added security updates for the following vulnerabilities: security updates CVE-2014-[0224, 0221, 0195, 3470, 0198, 1490, 1491, 1492, 1544, 1545, 5119, 0475, 3505, 3506, 3507, 3508, 3509, 3510, 3511, 3566, 1568], CVE-2010-5298, CVE-2012-5533, CVE-2013-1740. (S3)
25560 - Correctly handle FC switches with 256 or more outstanding credits. (S4)
27880 - Added a system message if customer contact information for call home is not set. Either the information should be set or Call Home should be disabled. (S4)
29912 - The web management application now uses a 2048-bit SSL RSA key instead of a 1024-bit key.
30888 - SNMP traps would intermittently change back to default after a system reboot. (S4)
25597 - The help for the CLI command "network DNS name server" now correctly displays usage of the "management controller" parameter. (S5)

29011 - The system log now contains a more informative message if the system fails to send Call Home information. (S5)

Release 6.3.1, patch 10

The following issue was fixed in version 6.3.1, patch 10:
30754 - Fixed erroneous interface DMA timeout that can occur approximately 497 days after boot. (S2)

Release 6.3.1, patch 9

The following issues were fixed in version 6.3.1, patch 9:
30000 - Trying to add a management controller back to the cluster after an unexpected crash could prevent future synchronization for configurations with a large number of access policies and/or logical units. This failure would result in stale information in the passive controller. (S1)
29528 - Any attempts to run SSH with a command would leave a process open and thus creating a memory leak. Since security scanners do this operation repeatedly, they could cause a management controller to crash. (S2)

Release 6.3.1, patch 8

The following issues were fixed in version 6.3.1, patch 8:
27565 - Added support for AIX6.1TL5 SFHA6.0.1
29084 - The dStroy feature is now available for erasing flashcards.
29056 - Using IBMi could result in stalled writes to the system. (S3)
28489 - When using access groups, removing logical units or access groups could result in stale information on the system. This would prevent users from being able to create new logical units with the same LUN. (S3)

Release 6.3.1, patch 5

The following issues were fixed in version 6.3.1, patch 5:
27255 - Applying a system patch after a live flashcard patch has been applied will cause an early shutdown, which could make components unresponsive. (S2)
27532 - Fixed InfiniBand controller issue where internal RAM timings would not be reset properly on boot and could lead to corrupted data. (S2)
26287 -The wear leveling algorithm has been modified to prevent a possible condition which could stall DMAs to the host. (S2)
24482 - Suppressed informational messages from SNMP in the system log. These debug level messages could cause system log overflow making the logs less useful. (S3)
26921 - If a FlashSystem port is set to Arbitrated Loop, direct-connecting to an HBA may take excessively long to link up. (S4)
27276 - In AIX environments with more than 32 Logical Units configured per host port, a fabric disruption could cause loss of access to the FlashSystem until the FlashSystem interfaces were reset or the FlashSystem was rebooted. (S4)
27325 - In AIX environments, SCSI recovery (Abort Task Set) may disrupt unrelated Logical Units, leading to unnecessary recovery on those Logical Units. (S4)

8.0 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 at http://www.ibm.com/planetwide/.

9.0 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 (® or ™), 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 on the Web at http://www.ibm.com/legal/copytrade.shtml.

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.