IBM Spectrum Scale advisories

Contents

Advisories for all platforms

Current advisories for all platforms

The following IBM Spectrum® Scale advisories affect all platforms:

Note: It is recommended that you are at the latest fix level available.

Attention: If you have V4.2.1 or V4.2.2.0 installed, you must migrate to V4.2.2.1 or later at your earliest convenience. For more information, see the Flash (Alert) here: http://www-01.ibm.com/support/docview.wss?uid=ssg1S1009965

- For V4.1.1 and later, see the flashes, alerts, and bulletins at https://www-947.ibm.com/support/entry/myportal/alerts/system_storage/storage_software/software_defined_storage/ibm_spectrum_scale?productContext=1538918429
- For V4.1 and prior, see the flashes, alerts, and bulletins for IBM Spectrum Scale at https://www-947.ibm.com/support/entry/myportal/alerts/cluster_software/general_parallel_file_system?productContext=444130266
- **IBM Spectrum Scale Alert : File encryption - encryption library change for Power7 and earlier models**

  Abstract:

  An internal change is being made to the encryption library used for file encryption, which may cause some performance impact on Power7 or earlier Power models.

  For more information, see https://www.ibm.com/support/pages/node/6343275.
- **IBM Spectrum Scale Alert for V4.2 and V5.0 levels: Files migrated from Spectrum Scale to external storage pools through DMAPI interfaces may cause undetected data corruption in snapshot files**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale V4.2.3.19 through 4.2.3.23 (ESS 5.2.9 through ESS 5.2.10), and V5.0.4.1 through 5.0.5.1 (ESS 5.3.5 through ESS 5.3.6 or ESS 6.0.0.0 through ESS 6.0.1.0) levels, in which files migrated from Scale to external storage pools through DMAPI interfaces may cause undetected data corruption in snapshot files.

  For more information, see https://www.ibm.com/support/pages/node/6262869.
- **IBM Spectrum Scale: Fixing QoS deadlock issue on QosPipeMutex requires IBM Spectrum Scale version upgrade**

  Problem:

  A Quality of Service (QoS) deadlock problem on QosPipeMutex might result in a cluster-wide deadlock impacting the cluster.

  For more information, see https://www.ibm.com/support/pages/node/1088998.
- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale where the local attacker can obtain root privilege by injecting parameters into setuid files (CVE-2019-4558)**

  Summary:

  A security vulnerability has been identified in all levels of IBM Spectrum Scale that could allow one to obtain root privilege by injecting parameters into setuid files. A fix for this vulnerability is available.

  For more information, see the complete bulletin at https://www.ibm.com/support/pages/node/1073732.
- **IBM Spectrum Scale (GPFS): Releases 4.2 or later have severe issues with file systems created by GPFS 2.2 or earlier releases**

  Abstract:

  IBM Spectrum Scale (GPFS) Release 4.2 support for file systems created by GPFS 2.2 or earlier releases: Version 4.2.3-16 or later addresses the previously reported issues with file systems created by GPFS 2.2 or earlier releases. Release 4.2.3 will be the last version of IBM Spectrum Scale that supports such older file systems, and Release 5.0.x will no longer support such file system format. A number of advanced functions are not supported with those file systems. You are advised to plan on migrating the data on those file systems into a new file system created by the 5.0 release to leverage features new to 5.0 levels.

  For more information, see the complete bulletin at https://www-01.ibm.com/support/docview.wss?uid=ibm10957131.
- **IBM Spectrum Scale Software/IBM Elastic Storage® Server: Release Recommendation**

  Abstract:

  IBM Spectrum Scale customers running prior versions are encouraged to upgrade to V4.2.3.14 in order to benefit from numerous quality improvement fixes included in this release. IBM Elastic Storage Server (ESS) V5.2.6 also leverages IBM Spectrum Scale V4.2.3.14 to provide additional robustness and reliability. IBM® also strongly recommends that ESS systems running prior versions be upgraded to ESS 5.2.6 or later releases.

  For more information, see the complete bulletin at http://www.ibm.com/support/docview.wss?uid=ibm10881942.

- **Flashes (Alerts): IBM Spectrum Scale (GPFS): Releases 4.2 or later have severe issues with file systems created by GPFS 2.2 or earlier releases**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale (GPFS) V4.2 through 5.0 in which mounting a file system created on GPFS 2.2 or earlier releases might result in the `mmfsd` daemon crashing when performing basic file system operations including creating files and writing to them. This is an old file system format as that release reached end-of-service in 2007.

  For more information, see the complete bulletin at http://www.ibm.com/support/docview.wss?uid=ibm10881468.
- **Flashes (Alerts): IBM Spectrum Scale (GPFS) V5.0.0.0 through 5.0.2.3: Off-line fsck repair on a file system with more than 32 sub-blocks per block may incorrectly repair duplicate reference corruptions, resulting in possible undetected data corruption or possible data loss**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale V5.0.0.0 through V5.0.2.3 code levels in which off-line fsck repair on a file system with more than 32 sub-blocks per block might incorrectly repair duplicate reference corruptions. This might result in undetected data corruption or in deletion of valid data blocks (data loss).

Note: This issue can occur only for file systems created at IBM Spectrum Scale V5.0.0.0 level (file system version 18.00) or later.

  For more information, see the complete bulletin at https://www-01.ibm.com/support/docview.wss?uid=ibm10875854.
- **Flashes (Alerts): IBM Spectrum Scale (GPFS) Version 4.1.x is going End Of Support on 4/30/2019**

  Abstract:

  End of support notification: IBM Spectrum Scale (GPFS) Version 4.1.x will reach End of Support on 2019-04-30.

  For more information, see the complete bulletin at http://www.ibm.com/support/docview.wss?uid=ibm10879357.
- **Flashes (Alerts): IBM Spectrum Scale (GPFS) 5.0 levels: reading files compressed with lz4 may result in daemon or kernel crashes, or possible undetected data corruption**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale (GPFS) V5.0.0 through 5.0.2.3 levels in which reading files compressed with lz4 from a node running V5.0.0 through 5.0.1.2 might result in daemon or kernel crashes. Attempts to uncompress the files might also result in errors or crashes (V5.0.0 through 5.0.1.2) or file system structure errors (5.0.2.0 through 5.0.2.3). Reading such compressed files might also result in undetected data corruption across any of the file systems.

  For more information, see the complete bulletin at https://www-01.ibm.com/support/docview.wss?uid=ibm10875682.
- **Flashes (Alerts): IBM Spectrum Scale (GPFS) V4.2 and 5.0 levels: a node or daemon failure may result in either data corruption in compressed files or undetected data corruption in snapshot files**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale (GPFS) V4.2 and V5.0 levels in which a node or daemon failure might result in either data corruption in compressed files or undetected data corruption in snapshot files.

  For more information, see the complete bulletin at http://www.ibm.com/support/docview.wss?uid=ibm10738705.
- **Flashes (Alerts): IBM has identified an issue in IBM Spectrum Scale (GPFS) V4.1, V4.2 and V5.0 levels, in which a node failure during file system restripe may result in silent data corruption or data loss in large files or file system structure errors**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale (GPFS) V4.1.1.0 through V4.1.1.22, V4.2.0.0 through V4.2.3.12, and V5.0.0.0 through V5.0.2.2 levels in which a node failure during file system restripe (`mmdeldisk`, `mmrestripefs`, `mmchdisk`, `mmrpldisk`, `mmdelsnapshot`, and `mmdelfileset`) might result in silent data corruption or data loss in large files or file system structure errors.

  For more information, see the complete bulletin at http://www.ibm.com/support/docview.wss?uid=ibm10869082.
- **Technote: IBM Spectrum Scale: Fix for deadlock may require file system format level to be updated**

  Problem:

  Failure to mount a file system in IBM Spectrum Scale 5.0.0 PTFs if the file system is created in (or upgraded to) 4.2.3 PTF9 (or later) or 4.1.1 PTF20 (or later). Failure to mount a file system in 4.2.3 PTF8 (or earlier) if the file system is created in (or upgraded to) 4.1.1 PTF20 (or later).

  For more information, see the complete technote at https://www-01.ibm.com/support/docview.wss?uid=ibm10719585.
- **Flashes (Alerts): IBM Spectrum Scale (GPFS): mismatched replicas with possible undetected data corruption following restripe operations (restripefs)**

  Problem Summary:

In a file system where data or metadata replication is used and "rapid repair" is enabled, and when there are "update in place" activities after disk(s) go down, followed by use of the `restripefs` command with options -r/-R/-m, mismatched replicas may be created after some disks are started up. Some replicas with stale data could result in metadata corruption in the file system, or data loss.

For more information, see the complete bulletin at http://www.ibm.com/support/docview.wss?uid=ibm10718849.

- **Flashes (Alerts): On IBM Spectrum Scale, when any of the quorum nodes are under high load, the cluster manager may unexpectedly lose its membership from the cluster resulting in unexpected cluster manager elections**

  Abstract:

  On IBM Spectrum Scale, when any of the quorum nodes are under high load, the cluster manager might unexpectedly lose its membership from the cluster resulting in unexpected cluster manager elections.

  For more information, see the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ibm10713707.

- **IBM Spectrum Scale Software/IBM Elastic Storage Server: Release Recommendation**

  Abstract:

  IBM Spectrum Scale customers running prior versions are encouraged to upgrade to V4.2.3.8 in order to benefit from numerous quality improvement fixes included in this release. IBM Elastic Storage Server (ESS) V5.2.2.1 also leverages IBM Spectrum Scale V4.2.3.8 to provide additional robustness and reliability. IBM also strongly recommends that ESS systems running prior versions be upgraded to ESS 5.2.2.1 or later releases.

  For more information, see the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1012386.

- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale with CES stack enabled that could allow sensitive data to be included with service snaps. This data could be sent to IBM during service engagements (CVE-2018-1512)**

  Summary:

  A security vulnerability has been identified in IBM Spectrum Scale with CES stack enabled that could allow sensitive data to be included with service snaps. This data could be sent to IBM during service engagements (CVE-2018-1512).

  For more information, see the complete security bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1012325.

- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale that could allow a local unprivileged user access to information located in dump files. User data could be sent to IBM during service engagements (CVE-2017-1654)**

  Summary:

  A vulnerability has been identified in IBM Spectrum Scale that could allow a local unprivileged user access to information located in dump files. User data could be sent to IBM during service engagements (CVE-2017-1654).

  For more information, see the complete security bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1010869.

- **Flash (Alert): IBM Spectrum Scale (GPFS) V4.1 and 4.2 levels: network reconnect function may result in file system corruption or undetected file data corruption**

  Abstract:

  IBM has identified a problem with IBM Spectrum Scale (GPFS) V4.1 and V4.2 levels. Resending an NSD RPC after a network reconnect function might result in file system corruption or undetected file data corruption.

  For more information, see the complete flash at http://www.ibm.com/support/docview.wss?uid=ssg1S1010668.

- **Flash (Alert): IBM Spectrum Scale (GPFS) V4.2.3: failures in scanning file system metadata may result in file system data or metadata corruption**

  Abstract:

  IBM has identified a problem with the GPFS file sys:tem metadata scanning function in IBM Spectrum Scale V4.2.3.0 through V4.2.3.3, which might result in silent file system data corruption or metadata corruption on certain failures.

  For more information, see the complete flash at http://www.ibm.com/support/docview.wss?uid=ssg1S1010487.

- **Flash (Alert): IBM Spectrum Scale (GPFS): On I/O with file size change on metanode takeover, the file size change may not be committed to disk**

  Abstract:

  IBM has identified an issue with IBM GPFS and IBM Spectrum Scale in which a file size change, which happens during a small timing window at the non-metanode, might not be committed to the disk during metanode takeover.

  For more information, see the complete flash at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1010293.

- **Flash (Alert): IBM Spectrum Scale: O_SYNC/O_DSYNC not honored, potentially causing some writes to be lost**

  Abstract:

  IBM has identified a problem with IBM Spectrum Scale V4.2.0.1 through V4.2.2.3, in which the O_SYNC/O_DSYNC flag to the open() system call could be ignored, which might result in undetected data corruption due to writes to the file (that appear to have been completed) being lost if a node failure occurs before data is written to disk.

For more information, see the complete flash at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1010130.

- **Technote: IBM Spectrum Scale Support: SKLM 2.7 UUID Length Workaround**

  Abstract:

  IBM Spectrum Scale versions up to and including 4.2.2.2 only support master encryption keys with identifiers up to 42 characters in length. With V2.7, IBM Security Key Lifecycle Manager (SKLM) generates encryption keys that are by default up to 48 characters long. Therefore, such keys cannot be used for encryption by IBM Spectrum Scale.

  For more information, see the complete technote at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1010026.

- **Flash (Alert): IBM Spectrum Scale V4.2.1/4.2.2 parallel log recovery function may result in undetected data corruption**

  Abstract:

  IBM identified a problem with the IBM Spectrum Scale parallel log recovery function in V4.2.1/V4.2.2, which might result in undetected data corruption during a file system recovery.

  For more information, see the complete flash at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1009965.

- **Security Bulletin: IBM Spectrum Scale and IBM GPFS are affected by a security vulnerability (CVE-2016-6115)**

  Summary: A security vulnerability has been identified in IBM Spectrum Scale (GPFS) that could allow a remote authenticated attacker to overflow a buffer and execute arbitrary code on the system with root privileges or cause the server to crash. This vulnerability is only applicable if:

  – file encryption is being used
  – the key management infrastructure has been compromised

  See the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1009639

- **Security Bulletin: A security vulnerability has been identified in GSKit shipped with IBM Spectrum Scale V4 (CVE-2016-2183)**

  Summary: A security vulnerability has been identified in one of the cipher suites supported by GSKit.

  See the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1009579

- **Abstract:**

  IBM Spectrum Scale and IBM GPFS are affected by security vulnerabilities (CVE-2016-2985 and CVE-2016-2984)

  Problem Summary:

  Security vulnerabilities have been identified in all levels of IBM Spectrum Scale and IBM GPFS that could allow:

  – a local attacker to execute commands as root by setting environment variables processed by setuid programs (CVE-2016-2985)
  – a local attacker to execute commands as root by supplying command line parameters to setuid programs (CVE-2016-2984)

  See the complete bulletin at either http://www.ibm.com/support/docview.wss?uid=ssg1S1007994 or http://www.ibm.com/support/docview.wss?uid=isg3T1023945

- **Abstract:**

  IBM Spectrum Scale and IBM GPFS are affected by a security vulnerability (CVE-2016-0392)

  Problem Summary:

  A security vulnerability has been identified in all levels of IBM Spectrum Scale and IBM GPFS that could allow a local attacker to inject commands into setuid file parameters and execute commands as root.

  See the complete bulletin at either http://www-01.ibm.com/support/docview.wss?uid=isg3T1023763 or http://www-01.ibm.com/support/docview.wss?uid=ssg1S1005781

- **Abstract:**

  IBM Spectrum Scale is affected by a security vulnerability (CVE-2015-7488)

  Problem Summary:

  A security vulnerability has been identified in the current levels of IBM Spectrum Scale V4.1.1 thru 4.1.1.3 and V4.2.0.0 that could allow a local, unprivileged user or a user with network access to the IBM Spectrum Scale cluster, access to the LDAP directory bind user password when File protocol is deployed with LDAP / LDAP with Kerberos based authentication.

  See the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1005580

- **Abstract: Multiple vulnerabilities in IBM Java™ SDK affect IBM Spectrum Scale (CVE-2015-4843, CVE-2015-4805, CVE-2015-4810, CVE-2015-4806, CVE-2015-4871, CVE-2015-4902)**

  Problem Summary:

  There are multiple vulnerabilities in IBM® SDK Java™ Technology Edition, Version 8 that is used by the IBM Spectrum Scale GUI. These issues were disclosed as part of the IBM Java SDK updates for October 2015.

  See the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1005579

- **Abstract:**

  IBM Spectrum Scale is affected by a security vulnerability (CVE-2015-7456)

  Problem Summary:

  A security vulnerability has been identified in the current levels of IBM Spectrum Scale V4.1.1 thru 4.1.1.3 and V4.2.0.0 that could allow a local unprivileged user, or a user with network access to the IBM Spectrum Scale cluster, to access admin passwords for object storage infrastructure. This vulnerability only affects clusters which have installed and deployed the Object protocol.

  See the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1005476
- **Abstract:**

  In an IBM Spectrum Scale V4.2 file system with multiple storage pools, Quality of Service (QoS) settings should be set for all storage pools to avoid performance degradation for unspecified storage pools.

  Problem Summary:

  In an IBM Spectrum Scale V4.2 file system with multiple storage pools, if the user specifies Quality of Service for I/O operations (QoS) settings (for the **maintenance** and **other** classes) only for one storage pool then the I/O allocations for the unspecified pools will be set to a very low value, resulting in severe performance degradation when I/O is performed to the unspecified storage pool(s).

  See the complete bulletin at http://www.ibm.com/support/docview.wss?uid=ssg1S1005464
- **Abstract:**

  IBM has identified a failure in the Spectrum Scale daemon which may occur when a given Network Shared Disk (NSD) object is deleted and then recreated via the mmdelnsd and mmcrnsd commands. When this failure occurs the Spectrum Scale mmfsd daemon will fail with the following assert message: logAssertFailed: cfgP->getNsdId() == cfgNP->getNsdId()

  Problem Summary:

  As a result of a timing hole that may occur in the propagation of changes to the configuration data, an mmfsd assert failure may occur after the mmcrnsd command is run for an NSD that was recently removed by the mmdelnsd command.

  See the complete bulletins at either http://www.ibm.com/support/docview.wss?uid=ssg1S1005460 or http://www.ibm.com/support/docview.wss?uid=isg3T1022972
- **Abstract:**

  A problem has been identified with AFM filesets using the NFS backend to communicate with a GPFS home that is running V4.1 or earlier when upgrading home to IBM Spectrum ScaleV 4.1.1 or later.

  Problem Summary:

  If there are AFM filesets using the NFS backend to communicate with a GPFS home that is running V4.1 or earlier, upgrading home to IBM Spectrum Scale V4.1.1 or later will cause the AFM filesets to disable synchronization to home with a message as follows: GPFS: 6027-3218 Change in home export detected. Synchronization with home is suspended until the problem is resolved. Please do not upgrade home from GPFS V4.1 or earlier to IBM Spectrum Scale V4.1.1 or later if continued AFM functionality is desired. Note: This only affects AFM filesets that were originally created with a GPFS home running V4.1 or earlier. This does not affect AFM filesets that were created with a home running IBM Spectrum Scale V4.1.1 or later.

  See the bulletins at either http://www.ibm.com/support/docview.wss?uid=ssg1S1005459 or http://www.ibm.com/support/docview.wss?uid=isg3T1022926
- **Security Bulletin: IBM Spectrum Scale and IBM GPFS are affected by security vulnerabilities (CVE-2015-4974, CVE-2015-4981)**

  Summary Security vulnerabilities have been identified in the current levels of IBM Spectrum Scale V4.1.1, IBM GPFS V4.1 and V3.5:

  - could allow a local non privileged attacker to execute commands with root privileges (CVE-2015-4974)
  - could allow a local non privileged attacker to read system memory contents (CVE-2015-4981)

  See the complete bulletin at either http://www-01.ibm.com/support/docview.wss?uid=ssg1S1005366 or http://www-01.ibm.com/support/docview.wss?uid=isg3T1022637
- **Security Bulletin: Vulnerability in OpenSSL affects IBM GPFS V4.1 and IBM Spectrum Scale V4.1.1 (CVE-2015-1788)**

  Summary: An OpenSSL denial of service vulnerability disclosed by the OpenSSL Project affects GSKit. IBM GPFS V4.1 and IBM Spectrum Scale V4.1.1 use GSKit and addressed the applicable CVE.

  See the complete bulletin at either http://www-01.ibm.com/support/docview.wss?uid=isg3T1022618 or http://www-01.ibm.com/support/docview.wss?uid=ssg1S1005364
- **Abstract:**

  IBM has identified a problem with the GPFS (IBM Spectrum Scale) Rapid Repair function, which is in use by default on GPFS 4.1 format file systems wherever data replication is in use, and may result in undetected data corruption.

  Problem Summary:

As a result of an incorrect calculation in GPFS code, an update to an internal data structure may result in modifications being made in the wrong memory location. If this location corresponds to a user data or metadata block, this block may become corrupted on disk. In addition, the same issue may result in back-level replicas of data blocks being present after recovery from down disks.

See the complete bulletins at either http://www-01.ibm.com/support/docview.wss?uid=isg3T1022582 or http://www-01.ibm.com/support/docview.wss?uid=ssg1S1005352

- **Abstract:**

  GPFS Product Support has received reports of errors accessing directories created since upgrading old GPFS file systems to use the new features of the V4.1 release. The issue is confined to the **rmdir** and **readdir** directory access paths on GPFS file systems originally created at the 3.1, or earlier, levels.

  Problem Summary:

  The DirV2 feature of GPFS V4.1 does not work correctly on file systems created prior to V3.2 (original format version less than 1000). Those early file systems use a different file name folding function (foldName) that does not support case-insensitive lookup for Windows (the key feature in V3.2, for these purposes), and DirV2 changes to hashing names within directory blocks does not handle this older foldName correctly. The two main effects of this problem are problems finding the ".." entry and properly sequencing **readdir** cookies. This leads to **rmdir** failing with **EEXIST** even when the direct is empty. It also causes directory enumeration with **readdir** (**getdents**) to repeat or skip entries and even to loop, repeatedly returning the same batch of names indefinitely. These problems only occur after updating the file system to V4.1 and only for directories created since the upgrade (i.e., only DirV2 directories).

  See the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=isg3T1022368
- **Security Bulletin: IBM General Parallel File System V4.1 is affected by a security vulnerability (CVE-2015-1890)**

  Summary: A security vulnerability has been identified in GPFS V4.1 where the private key of TLS client certificates used by GPFS nodes may be contained in a gpfs.snap file (CVE-2015-1890).

  See the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=isg3T1022077
- **Security Bulletin: IBM General Parallel File System is affected by security vulnerabilities (CVE-2015-0197, CVE-2015-0198, CVE-2015-0199)**

  Summary: Security vulnerabilities have been identified in current levels of GPFS V4.1, V3.5, and V3.4

  See the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=isg3T1022062
- **Abstract:**

  IBM has identified a problem with the online replica compare/repair function invoked via the **mmrestripefs -c** command.

  Problem Summary:

  IBM has identified a problem with the online replica compare/repair function invoked via the **mmrestripefs -c** command, when invoked with any disks having status other than **ready/replacement**, for example with any disks in **suspended** state. This function may cause file system corruption, with potential loss or corruption of user files, if any replica is be copied or moved for reasons other than replica mismatch. This problem affects customers running any PTF level of GPFS 3.5 from GPFS 3.5.0.11 through 3.5.0.20, or any level of IBM Spectrum Scale 4.1 from IBM Spectrum Scale 4.1.0.0 through IBM Spectrum Scale 4.1.0.3. The function provided by the **mmrestripefs -c** command is disabled in PTFs 3.5.0.21 and 4.1.0.4.

  Users affected :

  This problem affects customers running any PTF level of GPFS 3.5 from GPFS 3.5.0.11 through 3.5.0.20, or any level of IBM Spectrum Scale 4.1 from IBM Spectrum Scale 4.1.0.0 through IBM Spectrum Scale 4.1.0.3.

  This problem can only occur when the **mmrestripefs -c** command is run while there are disks with status other than **ready/replacement**. For a file system with data replication, the problem may only occur if none of the replicas of a data block are on a disk with status of **ready/replacement**.

  Users can check if they may have been affected by running the following command to determine if **mmrestripefs -c** was ever issued in the cluster:

  ```
  mmdsh -N all grep "mmrestripefs.*-c" /var/adm/ras/mmfs.log\*
  ```

  If the result of the grep indicates that the command has been run, contact IBM Service.

  Recommendation:

  - Avoid running the **mmrestripefs** command with the **-c** option until a fix is made available by IBM. A fix is made available for GPFS V3.5 with APAR IV66437 and IBM Spectrum Scale V4.1 with APAR IV66123.
  - Contact IBM for an efix to disable the code; APAR IV66270 for GPFS V3.5 and APAR IV66271 for IBM Spectrum Scale V4.1.
- **Abstract:**

  GPFS may incorrectly permit a disk that is too large for the file system to be added to an existing FPO storage pool, resulting in undetected data corruption of the file system

Problem Summary:

GPFS is designed to impose a maximum allowable disk size for disks added after the file system has been created. An integer overflow problem has been discovered in the GPFS block map allocation module that allows GPFS to incorrectly add disks too large to the file system. A disk that should have failed this maximum size check could be incorrectly added to an FPO enabled storage pool. If a disk is added with size equal to or larger than 8 times the size of the disks used at the time the file system was originally created and the file system is utilizing FPO enabled storage pools, data blocks will be corrupted when data is written to the new disk.

Users affected:

File systems that have added a disk or disks that are equal to or larger than 8 times the size of the disk used at the time the file system was originally created and GPFS has FPO enabled storage pools.

Please check the following conditions to assess if your file system is at risk:

1. Is the file system FPO enabled? Use the following command to determine. If it's yes, then this is a FPO pool.

   ```
   mmlspool fsname poolname -L | grep allowWriteAffinity
   ```

2. Is the file system metadata block size larger than 256KB? Use the following command to determine.

   ```
   mmlspool fsname system -L |grep blockSize
   ```

3. Have you added disks (or plan to add disks) to the file system that are equal to or larger than 8 times of the original disks via mmadddisk command? The new disks must be equal to or larger than 8 times in capacity than the largest disk existing at file system creation time. Use the following mmdf command to review sizes of disks belonging to the file system. Review the "disk size" column to determine disks that are equal to or larger than 8 times of size of the original disks in the file system.

   ```
   mmdf filesystem
   ```

   Below is an example from an affected system. The disk data01node04 was added after the file system was created and its size (3.5TB) is more than 8 times of the original largest disk size (296 GB).

   ```
   # mmdf gpfs1
   disk                disk size  failure holds    holds              free KB             free KB
   name                    in KB    group metadata data        in full blocks        in fragments
   --------------- ------------- -------- -------- ----- -------------------- -------------------
   Disks in storage pool: system (Maximum disk size allowed is 9.0 TB)
   data01node01        296874976     1001 yes      yes       293232640 ( 99%)          2144 ( 0%)
   data02node01        296874976     1001 yes      yes       293307392 ( 99%)          2784 ( 0%)
   data02node02        296874976     1002 yes      yes       296857600 (100%)          1984 ( 0%)
   data01node02        296874976     1002 yes      yes       296856576 (100%)          1984 ( 0%)
   data02node03        296874976     1003 yes      yes       293314560 ( 99%)          2784 ( 0%)
   data01node03        296874976     1003 yes      yes       293234688 ( 99%)          2144 ( 0%)
   data01node04       3512693760     1004 yes      yes      1306125312 ( 37%)     404892224 (12%)
                   -------------                         -------------------- -------------------
   (pool total)       5293943616                            3072928768 ( 58%)     404906048 ( 8%)
   ```

4. If you are still unable to determine, you will need to unmount the file system and run mmfsck. Please contact IBM support for assistance and further details to run mmfsck.

Problem Description:

See *Problem Summary*.

Required Actions:

IBM recommends that GPFS FPO enabled users apply a fix as soon as it is available and before adding new disks to the file system. For GPFS 3.5, the fix is available in GPFS 3.5.0.19 (IV60817) on Fix Central. For GPFS 4.1, the fix is available in GPFS 4.1.0.2 (IV62418) on the Fix Central site.

If you have determined that you are affected, please call IBM support as soon as possible for assistance with data recovery.

- **Abstract:**

  Conflicting advisory locks may result in undetected data corruption.

  Problem Summary:

  Conflicting advisory locks may be granted when applications use fcntl() to acquire advisory locks on a GPFS file. After a node acquires an advisory lock, if another node takes any action which triggers an inode token revoke (such as running the chmod command on the file), the fcntl token may be released while the fcntl lock is still held. If another application process then asks for a conflicting advisory lock for the same file, that request could be granted. User data could then be corrupted, because the two different application processes believe they have exclusive access to the same file range.

GPFS metadata will not be affected. Only customers using fcntl advisory locks at the affected GPFS levels could be impacted.

Users affected (both of the following conditions must apply for customer to be affected):

- Customers running GPFS service levels 4.1.0.0, or 4.1.0.1.
- Customer workload includes use of fcntl advisory locks on GPFS files.

Problem Description:

See *Problem Summary*.

Recommendation:

Affected customers should contact upgrade to V4.1.0.2 (APAR IV62043).

- **Abstract:**

IBM has identified an issue with GPFS version 3.5.0.16 and later releases that may affect installations that use both a non-English language locale settings and also have Persistent Reserve enabled for the cluster.

Problem Summary:

On such systems, it is possible that the disk usage information recorded in the main configuration file (/var/mmfs/gen/mmsdrfs) is not correct. This may result in an improper handling of the PR settings and inability to mount the affected file systems. The root cause for this problem is corrected in GPFS 3.5.0.19 and GPFS 4.1.0.1 (APAR IV61323)

Fix

To see if your system is susceptible to this problem, run the following command

```
grep SG_DISKS /var/mmfs/gen/mmsdrfs | awk -F : '{ print $3 " " $5 " " $8 }'
```

and examine the reported disk usage information. If you see **descOnly** shown for disks that are supposed to contain data or metadata, then your system is affected and you need to correct the problem using the following procedure:

1. install GPFS 3.5.0.19 or GPFS 4.1.0.1
2. for each of the affected file systems run

```
mmcommon recoverfs deviceName
```

If the **mmcommon recoverfs** command fails because it cannot read the file system descriptor, then you will need to temporarily disable the Persistent Reserve feature:

1. mmshtudown -a
2. mmchcconfig usePersistentReserve=no
3. mmstartup -a
4. mmcommon recoverfs *deviceName*

Note: repeat for all affected file systems

5. mmshtudown -a
6. mmchcconfig usePersistentReserve=yes
7. mmstartup -a

- **Abstract:**

GPFS directory corruption with possible undetected data corruption

Problem Summary:

When multiple nodes are updating a shared directory concurrently, the problem could cause incorrect results from directory operations issued on one node, leading to orphaned inodes (files inaccessible from any directory entry), or directory entries pointing to deleted or incorrect files. This problem could also cause silent data corruption, if any disk contains both GPFS metadata and data, and a stale buffer is written to a disk address that has been freed and reallocated for some other purpose.

Users affected (both of the following conditions must apply for customer to be affected):

- GPFS service levels 3.4.0.24, 3.4.0.25, 3.4.0.26, 3.4.0.27, 3.5.0.13. 3.5.0.14, 3.5.0.15, or 3.5.0.16.
- Workload consists of concurrent directory updates from multiple nodes.

Problem Description:

See https://www14.software.ibm.com/webapp/set2/subscriptions/onvdq?mode=7&heading=CL_CLUSTER&path=/201404/CL_GPFS/20140410/datafile123513&label=GPFS directory corruption with possible undetected data corruption

Recommendation:

Customers who have run the affected service levels should upgrade to GPFS 3.5.0.17 or 3.4.0.28 service level updates (go to Fix Central). Customers who have seen FSSTRUCT 1124 or 1122 messages, or EIO errors during directory operations, should also run off-line fsck to identify and repair possible directory damage.

- **Abstract:**

  A delete of a migrated file that has a copy in a snapshot will fail to recall the migrated data from HSM and the failure is not detected by GPFS.

  Problem:

  Under certain conditions, a delete of a migrated file that has a copy in a snapshot will fail to recall the migrated data from HSM and the failure is not detected by GPFS. A subsequent HSM reconcile operation initiated by the administrator may cause the HSM system to delete the last remaining copy of the file data that was thought to still remain on disk in the snapshot view.

  Root cause:

  The issue was discovered during testing of a scenario where many files were deleted from a file system that is managed by HSM. A GPFS snapshot of the file system had been created after HSM migration but before file deletion, so migrated files' data were not resident on disk. The deletion should cause a recall of each deleted file's data from the HSM to populate the snapshot view of the files. IBM is not aware of any occurrences of this issue in customer environments or under any other circumstances. Since the issue is specific to accessing only the snapshot copies of migrated data for already deleted files, it does not affect applications using the active (non-snapshot) view of the file system. If an administrator were to issue an HSM reconcile command, it is possible the HSM system may delete the last remaining copy of the file data for those files deleted, but believed to still be preserved in the GPFS snapshot.

  Fix:

  The fix is available in GPFS 3.5.0.18 (APAR IV58500) and GPFS 3.4.0.29 (APAR IV59300). Customers using HSM should update to 3.5.0.18 or 3.4.0.29 available on Fix Central.

  Users affected (all of the following conditions must apply for customer to be affected):

  Users of GPFS 3.4.0.16 and later, or GPFS 3.5.0.3 and later, who are utilizing HSM and the following conditions exist:

  – Files are migrated.
  – A GPFS snapshot is made of the file system.
  – Files are deleted from the active file system.
  – HSM Reconcile operation is initiated by the administrator.
  – Access of deleted files is attempted through the snapshot view of the file system.

- **Issue Description:**

  IBM has identified a memory leak in GPFS 3.5.0.14. Users of GPFS 3.5.0.14 may experience out of memory errors (ENOMEM) or a GPFS crash as a result of a memory allocation failure.

  Fix and Recommendations:

  IBM provided a fix for this problem now available in GPFS 3.5.0.15 (APAR IV51893). All customers using 3.5.0.14 should update to 3.5.0.15 or later, as soon as possible.

- **Abstract:**

  Under certain conditions, an issue with GPFS 3.5.0.10 - 3.5.0.12 using an AFM fileset may result in undetected in-memory data corruption.

  Issue Description:

  Under certain conditions involving an AFM fileset using any mode, a read to an uncached block in AFM cache while background prefetch is running may return wrong data (e.g., a buffer filled with zeros). The AFM background prefetch is triggered automatically when an application reads more than 2 blocks or based on the **afmPrefetchThreshold** value set on the fileset. The file data on disk is always correct, so a reread of the file will return correct data once background prefetch of the file completes.

  Users Affected:

  Only users of GPFS version 3.5.0.10 or later who are utilizing AFM cache and haven't explicitly disabled background prefetch.

  Users not Affected:

  – Users not running AFM.
  – GPFS users running 3.5.0.11 or later and having set **afmPrefetchThreshold** to 100.
  – GPFS users running AFM using 'SW' (Single Writer) mode, where all data is generated by the cache site (e.g. there are no read operations to the home cluster).

  Fix and Recommendations:

  The fix is available in GPFS 3.5.0.13 (APAR IV48136). Customers using AFM should update to 3.5.0.13 or later.

  Workaround until fix is applied:

Both of the below conditions must be met.

1. Set **afmPrefetchThreshold** to 100 (Note: requires GPFS 3.5.0.11 or later).
2. If the AFM prepop command (**mmafmctl** *Device* prefetch -j *FilesetName*) is running, ensure that the command completes before issuing writes to the fileset.

- **Abstract:**

  Under certain conditions, an issue with IBM GPFS 3.5.0.11 using AFM Single Writer or Independent Writer modes may result in undetected data loss.

  Issue Description:

  Under certain conditions involving an AFM fileset using Single Writer or Independent Writer modes, a write to an uncached block in the AFM cache may be overwritten by data subsequently arriving from the AFM home resulting in undetected data loss. This may occur when an application reads enough blocks of an uncached file to trigger AFM background prefetch, which will read data from home and write to cache. While this prefetch is running, an application write to an uncached portion of the file (file blocks not yet pre-fetched to the AFM cache) may succeed, but at a later point the block so written may be overwritten with data from the AFM home which had not yet arrived in the AFM cache.

  Users Affected:

  Only users of GPFS version 3.5.0.11 who are utilizing AFM Single Writer or Independent Writer cache starting with non-empty AFM home.

  Users not Affected:

  The following uses of GPFS version 3.5.0.11 should not be affected by this issue.

  1. Users not running AFM
  2. Read Only or Local Update AFM caches
  3. Single Writer or Independent Writer AFM caches with empty AFM home
  4. Files created in AFM Single Writer or Independent Writer caches

  Fix and Recommendations:

  The fix is available in GPFS 3.5.0.12 (APAR IV46085). Customers using AFM should update to 3.5.0.12 or later.

  Workaround until fix is applied:

  Both of the below conditions must be met.

  1. Set afmPrefetchThreshold to 100
  2. If the AFM prepop command (**mmafmctl** *Device* prefetch -j *FilesetName*) is running, ensure that the command completes before issuing writes to the fileset.

- In internal testing on an unsupported configuration, IBM has identified a potential data integrity issue in GPFS 3.4.0.9 and later releases of GPFS 3.4, and with GPFS 3.5. This issue has not, to IBM's knowledge, been experienced in the field. The issue occurs only when writing via NFS to a GPFS node running on the Linux® operating system. This issue may manifest as either a data loss issue from a transient read error, returning zeros rather than the expected data, or as incorrect data returned following a write that is applied to the wrong file.

  The fix for this issue is in GPFS 3.4.0.15 (APAR IV24937) and GPFS 3.5.0.3 (APAR IV24942). While IBM cannot rule out the possibility that this problem may impact any customer writing via NFS in Linux GPFS environments at the stated levels, empirical evidence suggests that the likelihood of customers encountering this issue is quite limited. To avoid this issue customers should upgrade to GPFS 3.4.0.15 or GPFS 3.5.0.3 or later.

- IBM has identified an issue with GPFS file systems at version 3.5 which currently use, or have previously used independent filesets and Access Control Lists (ACLs). This issue can occur if independent filesets have been created with the **mmcrfileset --inode-space** command and any files or directories in the GPFS file system have ACLs added or modified with commands such as **mmputacl** or **mmeditacl**. File systems which have previously used but have now deleted independent filesets are still susceptible to this issue.

  The issue can result in a loss of data access to any file or directory within the GPFS file system which has an ACL.

  The fix is available in GPFS version 3.5.0.3 (APAR IV24426).

  Customers who have created independent filesets, even if the filesets are now deleted, are requested to not create or modify GPFS ACLs on any file or directory until the IBM Service fix is applied.

  Customers who have not created independent filesets are requested to not do so until the IBM Service fix is applied.

  If you are already affected by loss of access to files or directories with ACLs, then you are requested to call IBM Service and reference this problem. The IBM Service person will walk you through a fix for correcting the issue.

  Please follow the steps below to determine if your GPFS file system may be susceptible to this issue.

  1. On a system with GPFS running, invoke the **mmlsconfig** command to determine the device names of all file systems

2. For each file system device listed in step 1, use the following command to determine if your system may be affected:

   ```
   echo desc | /usr/lpp/mmfs/bin/tsdbfs fs-device | grep inodeSpaceMask
   ```

   where *fs-device* is the device output from step 1 (e.g. /dev/gpfs in step 1 output example)

   If there is any non-zero value from the output of the command, your system is exposed to the issue.

   In the following example, the file system **/dev/gpfs** is safe (no independent filesets were created) but files in file system **/dev/trouble** with ACLs are at risk.

   ```
   # echo desc | /usr/lpp/mmfs/bin/tsdbfs /dev/trouble | grep inodeSpaceMask
       inodeSpaceMask 0000000000000100 0000000000000000000000000000000000000000000000000000000100000000

       # echo desc | /usr/lpp/mmfs/bin/tsdbfs /dev/gpfs | grep inodeSpaceMask
       inodeSpaceMask 0000000000000000 0000000000000000000000000000000000000000000000000000000000000000
   ```

- IBM has identified an issue with GPFS file systems at versions 3.4 or 3.5 which were migrated from file systems created with GPFS versions earlier than 3.4. This issue can occur only after using the **mmmigratefs** command with the **[--fastea]** option.

  The issue can result in a loss of data, requiring the restoration of data from a backup source.

  GPFS file systems created with versions earlier than 3.4 should not be migrated using the **mmmigratefs** command with the **[--fastea]** option unless you are at GPFS version 3.5.0.3 (APAR IV24151) or later, or 3.4.0.15 (APAR IV24150) or later.

  If customers have already migrated file systems from GPFS versions earlier than 3.4, IBM Service has a fix. Please follow the steps below to determine if your system may be affected.

  To determine if your system may be affected:

  1. Ensure your GPFS file systems are mounted.
  2. As a user with GPFS administrator privileges on a machine where your GPFS file systems are mounted, issue the command:

     ```
       /usr/lpp/mmfs/bin/mmfsadm dump stripe | grep "inode 0"
     ```

     The command will produce output that identifies locations for the "inode 0" file for all currently mounted GPFS file systems. Example output for a file system configured with two way metadata replication would be in the form:

     ```
      inode 0: 3:4098 1:4098
     ```

     For a file system with no metadata replication the output would be in the form:

     ```
        inode 0: 3:4098
     ```

     The relevant information to look for to see if you may experience a problem are the fields denoting *disk*:*sector* for each inode 0 replica (e.g. 3:4098 and 1:4098 in these examples).

     If each *disk*:*sector* replica only denotes 4098 for the sector field then you are not experiencing this problem. **If however there is a number other than 4098 in the sector output then you are requested to immediately call IBM service and reference this problem.** The IBM Service person will walk you through a fix for correcting the issue.

- When installing or migrating GPFS, the minimum levels of service you must have applied are:

  – GPFS V3.5 you must apply APAR IV15333 (GPFS V3.5.0.1)
  – GPFS V3.4 you must apply APAR IZ78460 (GPFSV3.4.0.1)

  If you do not apply these levels of service and you attempt to start GPFS, you will receive an error message similar to:

  ```
  mmstartup: Required service not applied. Install GPFS 3.5.0.1 or later
  mmstartup: Command failed Examine previous error messages to determine cause
  ```

Advisories for AIX

Current advisories for AIX

The following IBM Spectrum Scale advisories affect AIX®:

- **IBM Spectrum Scale Alert for V4.2 and V5.0 levels: Files migrated from Spectrum Scale to external storage pools through DMAPI interfaces may cause undetected data corruption in snapshot files**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale V4.2.3.19 through 4.2.3.23 (ESS 5.2.9 through ESS 5.2.10), and V5.0.4.1 through 5.0.5.1 (ESS 5.3.5 through ESS 5.3.6 or ESS 6.0.0.0 through ESS 6.0.1.0) levels, in which files migrated from Scale to external storage pools through DMAPI interfaces may cause undetected data corruption in snapshot files.

  For more information, see https://www.ibm.com/support/pages/node/6262869.
- **IBM Spectrum Scale Alert for V4.2 and V5.0 levels: write operations doing direct I/O may cause undetected data corruption in snapshot files**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale V4.2.0.0 through 4.2.3.21 (ESS 4.0 through ESS 5.2.9), and V5.0.0.0 through 5.0.4.3 (ESS 5.3 through ESS 5.3.5.2 or ESS 6.0.0.0 through ESS 6.0.0.2) levels, in which write operations doing direct I/O (files opened with the O_DIRECT flag) may cause undetected data corruption in snapshot files.

  For more information, see https://www.ibm.com/support/pages/node/6234994.
- **IBM Spectrum Scale V4.2 and V5.0 levels: possible undetected data corruption on compressed file**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale V4.2.0.0 through 4.2.3.21 (ESS 4.0 through ESS 5.2.9), or V5.0.0.0 through 5.0.4.3 levels (ESS 5.3 through ESS 5.3.5.2 or ESS 6.0.0.0 through ESS 6.0.0.2), in which undetected data corruption may occur for data being written with small sequential write (non-direct I/O) operations, while a file is being concurrently compressed or decompressed.

  For more information, see https://www.ibm.com/support/pages/node/6220548.
- **IBM Spectrum Scale(GPFS) Alert for V4.2 and V5.0 levels: possible silent data corruption may happen on snapshot files.**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale (GPFS) V4.2.0.0 through 4.2.3.19 (ESS 4.0 through ESS 5.2.8), and V5.0.0.0 through 5.0.4.2 (ESS 5.3 through ESS 5.3.5.1)levels, in which undetected data loss or corruption may result from incorrect data being read from snapshot files, after a snapshot deletion or while operations involving data copy-on-write to latest snapshot files are in progress.

  For more information, see https://www.ibm.com/support/pages/node/6213729.
- **IBM Spectrum Scale (GPFS) Alert : Versions prior to 5.0.4.2 (ESS 5.3.5.1 and ESS 6.0.0.1) are affected by an issue in offline fsck which may result in metadata or data loss.**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale (GPFS), versions prior to 5.0.4.2, in which offline fsck may fail to report and repair duplicate reference corruption present in the inode 0 files of an active file system and snapshots of that file system, resulting in loss of data or metadata or undetected data corruption.Refer to the "GPFS architecture" section in the "Concepts, Planning, and Installation Guide" for a description of inode 0 file a.k.a inode file.

  For more information, see https://www.ibm.com/support/pages/node/5736741.
- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale where an unprivileged user to cause denial of service in kernel (CVE-2020-4411)**

  Summary:

  A security vulnerability has been identified in all levels of IBM Spectrum Scale that could allow a local attacker to cause a denial of service. A fix for this vulnerability is available.

  For more information, see https://www.ibm.com/support/pages/node/6209002.
- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale where an unprivileged user to cause denial of service(CVE-2020-4412)**

  Summary:

  A security vulnerability has been identified in all levels of IBM Spectrum Scale that could allow a local attacker to cause a denial of service. A fix for this vulnerability is available.

For more information, see https://www.ibm.com/support/pages/node/6209004.

- **IBM Spectrum Scale (GPFS) Alert : Multiple NFS-Ganesha issues may end up using freed memory leading to a crash or a hang.**

  Abstract:

  NFS-Ganesha shipped in IBM Spectrum Scale V5.0.4.0 to V5.0.4.3 may end up using freed memory leading to a crash or a hang while trying to re-use in-memory chunking data structure as part of executing a directory listing (NFS READDIR) request.

  For more information, see https://www.ibm.com/support/pages/node/6207920.
- **IBM Spectrum Scale(GPFS) Alert for V4.2 and V5.0 levels: data corruption may happen on compressed files.**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale (GPFS) V4.2.0.0 through 4.2.3.20 (ESS 4.0 through 5.2.9), and V5.0.0.0 through 5.0.4.2 (ESS 5.3 through 5.3.5.1) levels, in which the concurrent use of mmap write and compression operations may cause the data in data blocks being compressed to be corrupted.

  For more information, see https://www.ibm.com/support/pages/node/5736753.
- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale where an unprivileged user could execute commands as root (CVE-2020-4273)**

  Summary:

  A security vulnerability has been identified in all levels of IBM Spectrum Scale that could allow an underprivileged attacker to execute commands as root. A fix for this vulnerability is available.

  For more information, see https://www.ibm.com/support/pages/node/6151701.
- **IBM Spectrum Scale (GPFS) 4.2.3 (ESS 5.2) and 5.0 (ESS 5.3) levels Alert: command "mmchdisk start" may succeed without synchronizing the replicas and may result in undetected data corruption.**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale (GPFS) V4.2.0.0 through V4.2.3.18 (ESS 4.0 through ESS 5.2.8) and V5.0.0.0 through V5.0.4.1 (ESS 5.3 through ESS 5.3.5) in which, in a replicated file system, the command `mmchdisk <file system> start` might indicate success even without being able to synchronize all the replicas. That might result in undetected data corruption, as attempts to read files might retrieve data from an out-of-date or uninitialized replica. One known scenario where the command is unable to synchronize all the replicas but still indicates success happens in an encrypted file system, when problems occur in accessing the key servers while the command is being processed.

  For more information, see https://www.ibm.com/support/pages/node/3555453.
- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale where an attacker can cause a denial of service (CVE-2020-4217)**

  Summary:

  A security vulnerability has been identified in all levels of IBM Spectrum Scale that could allow an attacker to cause a denial of service. A fix for this vulnerability is available.

  For more information, see https://www.ibm.com/support/pages/node/5693463.
- **IBM Spectrum Scale (GPFS) 5.0.4 levels: possible metadata or data corruption during file system log recovery**

  Abstract:

  IBM has identified a problem with the IBM Spectrum Scale parallel log recovery function at V5.0.4.0 - V5.0.4.1, which might result in metadata corruption or undetected data corruption during the course of a file system recovery.

  For more information, see https://www.ibm.com/support/pages/node/1274428.
- **IBM Spectrum Scale Active File Management (AFM) issues which may result in undetected data corruption.**

  Abstract:

  IBM has identified issues affecting Active File Management (AFM) in IBM Spectrum Scale V5.0.0.0 through V5.0.4.1, which might result in undetected data corruption.

  For more information, see https://www.ibm.com/support/pages/node/1172272.
- **IBM Spectrum Scale (GPFS): Avoid using mmrestripefs -c to repair replicas.**

  Abstract:

  IBM recommends that users not invoke the command `mmrestripefs -c` to compare and fix data and metadata replicas, as in some cases this might result in copying bad replica data to formerly good replicas.

  For more information, see https://www.ibm.com/support/pages/node/1114845.
- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale where remote authenticated attacker can execute arbitrary command(CVE 2019-4715)**

Summary:

A security vulnerability has been identified in all levels of IBM Spectrum Scale that could allow remote authenticated attacker to execute arbitrary command on the system. This vulnerability only affects systems where the SMB protocol is enabled. A fix for this vulnerability is available.

For more information, see https://www.ibm.com/support/pages/node/1118913.

- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale which allows users to embed arbitrary JavaScript code in the Web UI (CVE-2019-4665)**

  Summary:

  A security vulnerability has been identified in all levels of IBM Spectrum Scale that could allow users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. A fix for this vulnerability is available.

  For more information, see https://www.ibm.com/support/pages/node/1118937.
- **Flashes (Alerts): IBM Spectrum Scale (GPFS) 4.2.3 and 5.0 levels: concurrent mmap and read from the same files may result in undetected data corruption**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale (GPFS) V4.2.3.15 through 4.2.3.16, and V5.0.3.0 through 5.0.3.2 levels, in which concurrent read and mmap operations on the same file by multiple processes or threads might result in undetected data corruption in the form of a read operation returning incorrect data.

  For more information, see the complete bulletin at https://www-01.ibm.com/support/docview.wss?uid=ibm10960396.
- **Technote (Troubleshooting): IBM Spectrum Scale: Vormetric DSM V6.0.2, V6.0.3 and V6.1.x releases are not supported with IBM Spectrum Scale Encryption**

  Problem:

  Vormetric DSM V6.0.2, V6.0.3, and V6.1.x user interface do not support creation of KMIP objects such as the Master Encryption Keys (MEKs) used by IBM Spectrum Scale encryption, and as a result, IBM Spectrum Scale encryption cannot use these DSM releases.

  For more information, see the complete technote at https://www-01.ibm.com/support/docview.wss?uid=ibm10734479.
- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale that could allow a local, unprivileged user to cause a kernel panic (CVE-2018-1782)**

  Summary:

  IBM Spectrum Scale could allow a local, unprivileged user to cause a kernel panic on a node running IBM Spectrum Scale by accessing a file that is stored on an IBM Spectrum Scale file system with `mmap`, or by executing a crafted file stored on an IBM Spectrum Scale file system.

  For more information, see the complete bulletin at https://www-01.ibm.com/support/docview.wss?uid=ibm10730967.
- **Flashes (Alerts): IBM Spectrum Scale Active File Management (AFM) and AFM Asynchronous Disaster Recovery (ADR) issues, which may result in undetected data corruption**

  Abstract:

  IBM has identified certain issues affecting Active File Management (AFM) and AFM Asynchronous Disaster Recovery (ADR) in IBM Spectrum Scale, which might result in undetected data corruption.

  1. AFM might intermittently read files from the home cluster incorrectly if the replication factor is more than one at the cache cluster, which might result in undetected data corruption.
  2. AFM cache might incorrectly read an HSM migrated file from the home cluster due to the incorrect calculation of the file sparseness information, which could potentially result in undetected data corruption.
  3. AFM `mmafmctl Device resync/failover` and AFM ADR `mmafmctl Device changeSecondary` commands might miss copying data to the home or secondary cluster (from the other cluster) when the in-memory queue is dropped with pending in-place writes.
  4. AFM Asynchronous Disaster Recovery (ADR) could cause some files to be missing from the RPO snapshot at the secondary if recovery was run from the recovery+RPO snapshot.
  5. AFM might not replicate the data when the `dm_write_invis()` API is used to write. In addition, the `dm_read_invis()` API might read incorrect data if the file is not already cached.

  For more information, see the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ibm10713675.
- **IBM Spectrum Scale Software/IBM Elastic Storage Server: Release Recommendation**

  Abstract:

  IBM Spectrum Scale customers running prior versions are encouraged to upgrade to V4.2.3.8 in order to benefit from numerous quality improvement fixes included in this release. IBM Elastic Storage Server (ESS) V5.2.2.1 also leverages IBM Spectrum Scale V4.2.3.8 to provide additional robustness and reliability. IBM also strongly recommends that ESS systems running prior versions be upgraded to ESS 5.2.2.1 or later releases.

For more information, see the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1012386.

- **Security Bulletin: Vulnerabilities in GSKit affect IBM Spectrum Scale (CVE-2018-1431, CVE-2017-3736, CVE-2017-3732, CVE-2016-0705)**

  Summary:

  Vulnerabilities in GSKit affect IBM Spectrum Scale where:

  – A local attacker could obtain control of the IBM Spectrum Scale daemon to access and modify files in the IBM Spectrum Scale file system, and possibly to obtain administrator privileges on the node (CVE-2018-1431).
  – OpenSSL could allow a remote attacker to obtain sensitive information, which is caused by a carry propagation flaw in the x86_64 Montgomery squaring function bn_sqrx8x_internal(). An attacker with online access to a system that is not patched could exploit this vulnerability to obtain information about the private key (CVE-2017-3736).
  – OpenSSL could allow a remote attacker to obtain sensitive information, which is caused by a carry propagating bug in the x86_64 Montgomery squaring procedure. An attacker could exploit this vulnerability to obtain information about the private key (CVE-2017-3732).
  – OpenSSL is vulnerable to a denial of service, which is caused by a double-free error when parsing DSA private keys. An attacker could exploit this vulnerability to corrupt memory and cause a denial of service (CVE-2016-0705).

  For more information, see the complete security bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1012049.

- **Technote (troubleshooting): IBM Spectrum Scale support: mmchfs -V full command will fail on upgrade from file system 2.2**

  Problem (Abstract):

  If your file system version is still at the 2.2 level, then running mmchfs -V full on certain levels of IBM Spectrum Scale will cause the mmchfs command to fail. The file system will be unusable until the fix is applied.

  For more information, see the complete technote at http://www.ibm.com/support/docview.wss?uid=ssg1S1010654.

- **Flash (Alert): IBM Spectrum Scale (GPFS) AFM incorrectly replicates data when write and truncate operations are interleaved**

  Abstract:

  IBM has identified an issue with AFM in IBM GPFS (V3.5.0.0 through V3.5.0.34 or V4.1.0.0 through V4.1.0.8) and IBM Spectrum Scale (V4.1.1.0 through V4.1.1.16 or V4.2.0.0 through V4.2.3.4) levels where AFM might not transfer write operations completely when a file is truncated. This might cause a data mismatch between cache (or primary) and home (or secondary). This issue might result in undetected data corruption at home (or secondary).

  For more information, see the complete flash at http://www.ibm.com/support/docview.wss?uid=ssg1S1010629.

- **Flash (Alert): IBM Spectrum Scale v4.2.3.1 and v4.2.3.2 installation toolkit on ppc64 platform(/usr/lpp/mmfs/4.2.3.x/installer/spectrumscale) might fail when attempting to run ./spectrumscale install, deploy, or upgrade**

  Abstract:

  IBM has identified an issue with IBM Spectrum Scale v4.2.3.1 and v4.2.3.2 of the installation toolkit on ppc64 in which the toolkit might fail if it is run multiple times. This can occur during install, deploy, or upgrade and will give a FATAL message to the user and prevent the desired task from completing.

  For more information, see the complete flash at http://www.ibm.com/support/docview.wss?uid=ssg1S1010505.

- **Flash (Alert): IBM Spectrum Scale: AFM incorrectly replicates rename operations**

  Abstract:

  IBM has identified an issue with AFM in IBM Spectrum Scale V4.1.1.12 through V4.1.1.15 and V4.2.2.0 through V4.2.3.2 levels where AFM might incorrectly replicate the rename operations. This issue might cause undetected data loss due to some files missing at the target site.

  For more information, see the complete flash at http://www.ibm.com/support/docview.wss?uid=ssg1S1010426.

- **Flash (Alert): IBM Spectrum Scale (GPFS) V4.2.3 AFM with DMAPI-enabled file system causes mmfsd daemon failure on gateway node**

  Abstract:

  IBM identified an issue with AFM on a DMAPI-enabled filesystem in IBM Spectrum Scale V4.2.3 where health monitoring is enabled by default, which causes an mmfsd daemon assert on the gateway node. This issue might cause the mmfsd daemon on the gateway nodes to fail and restart repeatedly.

  For more information, see the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1010103.

- **Flash (Alert): IBM Spectrum Scale Active File Management (AFM) and AFM Asynchronous Disaster Recovery (DR)**

  Abstract:

IBM identified certain situations with respect to Active File Management (AFM) and AFM Asynchronous Disaster Recovery (DR) in IBM Spectrum Scale that may result in undetected data corruption:

- AFM may intermittently read files from the home cluster incorrectly, which could result in undetected data corruption due to Direct IO usage.
- AFM may have undetected data corruption when eviction and read operations run in parallel on the same file.
- AFM cache may incorrectly read a file from the home cluster due to the incorrect calculation of the file sparseness information, potentially resulting in undetected data corruption.
- If parallel IO is enabled, AFM and AFM Asynchronous DR may experience undetected data corruption with failover, resync and changeSecondary commands.
- AFM Asynchronous DR failback may read HSM migrated files from the acting AFM Primary cluster (originally the AFM Secondary cluster) as sparse files, potentially resulting in the AFM cache to return incorrect data (all zeros) to an application on a read.

See the complete bulletin at either http://www-01.ibm.com/support/docview.wss?uid=ssg1S1009244 or http://www-01.ibm.com/support/docview.wss?uid=isg3T1024249.

- **Flash (Alert): IBM Spectrum Scale (GPFS) V4.2 and V4.1.1 AFM Async DR requirement for planning**

  Abstract:

  Our initial feedback from the field suggests that success of a disaster recovery solution depends on administration discipline, including careful design, configuration and testing. Considering this, IBM has decided to disable the Active File Management- based Asynchronous Disaster Recovery feature (AFM DR) by default and require that customers deploying the AFM DR feature first review their deployments with IBM Spectrum Scale development. You should contact Spectrum Scale Support at scale@us.ibm.com to have your use case reviewed. IBM will help optimize your tuning parameters and enable the feature. Please include this message while contacting IBM Support.

  See the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1005817

- **Flash (Alert): IBM Spectrum Scale (GPFS) V4.2 AFM cache reads an HSM migrated file from home as a sparse file**

  Abstract:

  IBM has identified an issue with AFM in IBM Spectrum Scale V4.2.0.0 through 4.2.0.2 levels when the AFM cache reads the HSM migrated files from home (running IBM Spectrum Scale V4.2 or later) as a sparse file. This issue may cause the cache to have undetected data corruption and may return incorrect data (all zeros) to an application on read.

  See the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1005766

- **Security Bulletin: IBM Spectrum Scale is affected by a security vulnerability (CVE-2016-0263)**

  Summary:

  A security vulnerability has been identified in the current levels of IBM Spectrum Scale V4.2, V4.1 and IBM General Parallel File System V3.5, that could allow a local user, under special circumstances, to escalate their privileges or cause a denial of service when the mmapplypolicy command is issued with certain options and syntax.

  See the complete bulletin at either http://www-01.ibm.com/support/docview.wss?uid=isg3T1023450 or http://www-01.ibm.com/support/docview.wss?uid=ssg1S1005708

- **Security Bulletin: IBM Spectrum Scale V4.1.1, IBM GPFS V4.1, and IBM V3.5 for AIX are affected by a security vulnerability (CVE-2015-7403)**

  Summary:

  A security vulnerability has been identified in the current levels of IBM Spectrum Scale V4.1.1, IBM GPFS V4.1 and V3.5 that could allow a local attacker to cause the node they are on to crash.

  See the complete bulletin at either http://www-01.ibm.com/support/docview.wss?uid=ssg1S1005452 or http://www.ibm.com/support/docview.wss?uid=isg3T1022940

- In order for tracing to function properly on a system running the levels of AIX listed below, appropriate service must be installed. If you are running GPFS without the appropriate service level installed and have AIX tracing enabled (such as by using the GPFS **mmtracectl** command), you will experience a GPFS memory fault (coredump) or node crash with kernel panic.

  - AIX V7.1 with the 7100-00 Technology Level, you must either install AIX 7100-00-02 Service Pack or open a PMR to obtain an iFix for APAR IZ84576 from IBM Service.
  - AIX V6.1 with the 6100-06 Technology Level, you must either install AIX 6100-06-02 Service Pack or open a PMR to obtain an iFix for APAR IZ84729 from IBM Service.

Advisories for Linux

Current advisories for Linux

The following advisories affect Linux:

- **IBM Spectrum Scale Alert : Active AFM DR Relationships goes to the Unmounted state.**

  Abstract:

  Upgrading to IBM Spectrum Scale versions 5.0.5.4 (or) 5.1.0.1 from 5.0.5.2 (or) 5.0.5.3 (or) 5.1.0.0 might push previously Active AFM DR Relationships to the Unmounted state - halting data replication from the Production site to the DR Site.

  For more information, see https://www.ibm.com/support/pages/node/6380740.
- **IBM Spectrum Scale Alert for V5.1.0.0 level: Cascaded failure of manager nodes on clusters when more than 64 nodes fail simultaneously or are shutdown.**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale V5.1.0.0 in which, if more than 64 nodes simultaneously fail or lose quorum, it can result in the file system manager failing with the assertion "`logAssertFailed: nFailedNodes <= 64`". This can then trigger cascaded failure of manager nodes and result in loss of cluster membership and/or the file system unmounting.

  For more information, see https://www.ibm.com/support/pages/node/6380738.
- **IBM Spectrum Scale Alert : File encryption - client and server certificate(s) expiration, result in loss of access to the encrypted files.**

  Abstract:

  IBM Spectrum Scale Encryption uses certificates to authenticate a connection between a key client and a key server. A key client certificate and key server certificate will expire some time after configuring encryption, resulting in loss of access to the encrypted files.

  For more information, see https://www.ibm.com/support/pages/node/6369269.
- **IBM Spectrum Scale Alert : `mmfsck` command option causes new mount failure**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale V5.0.4.0 through V5.0.4.4, and V5.0.5.0 through V5.0.5.3 (ESS 5.3.5 through ESS 5.3.6.1 or ESS 6.0.0.0 through ESS 6.0.1.1) code levels, in which using the --estimate-only option of `mmfsck` while the file system is online causes new mounts to fail and other data access problems.

  For more information, see https://www.ibm.com/support/pages/node/6365005.
- **IBM Spectrum Scale Alert for V4.2 and V5.0 levels: Files migrated from Spectrum Scale to external storage pools through DMAPI interfaces may cause undetected data corruption in snapshot files**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale V4.2.3.19 through 4.2.3.23 (ESS 5.2.9 through ESS 5.2.10), and V5.0.4.1 through 5.0.5.1 (ESS 5.3.5 through ESS 5.3.6 or ESS 6.0.0.0 through ESS 6.0.1.0) levels, in which files migrated from Scale to external storage pools through DMAPI interfaces may cause undetected data corruption in snapshot files.

  For more information, see https://www.ibm.com/support/pages/node/6262869.
- **IBM Spectrum Scale Alert: HDFS Transparency version 3.1.0-4 or version 3.1.1-0 have NameNode hang issue**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale HDFS Transparency version 3.1.0-4 or version 3.1.1-0 where the NameNode can hang intermittently.

  For more information, see https://www.ibm.com/support/pages/node/6256542.
- **IBM Spectrum Scale Alert for V4.2 and V5.0 levels: write operations doing direct I/O may cause undetected data corruption in snapshot files**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale V4.2.0.0 through 4.2.3.21 (ESS 4.0 through ESS 5.2.9), and V5.0.0.0 through 5.0.4.3 (ESS 5.3 through ESS 5.3.5.2 or ESS 6.0.0.0 through ESS 6.0.0.2) levels, in which write operations doing direct I/O (files opened with the O_DIRECT flag) may cause undetected data corruption in snapshot files.

  For more information, see https://www.ibm.com/support/pages/node/6234994.
- **IBM Spectrum Scale V4.2 and V5.0 levels: possible undetected data corruption on compressed file**

Abstract:

IBM has identified an issue in IBM Spectrum Scale V4.2.0.0 through 4.2.3.21 (ESS 4.0 through ESS 5.2.9), or V5.0.0.0 through 5.0.4.3 levels (ESS 5.3 through ESS 5.3.5.2 or ESS 6.0.0.0 through ESS 6.0.0.2), in which undetected data corruption may occur for data being written with small sequential write (non-direct I/O) operations, while a file is being concurrently compressed or decompressed.

For more information, see https://www.ibm.com/support/pages/node/6220548.

- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale GUI where an unauthorised user can execute commands (CVE-2020-4348)**

  Summary:

  A security vulnerability has been identified in all levels of IBM Spectrum Scale GUI that could allow an unauthorised user to execute commands . A fix for this vulnerability is available.

  For more information, see https://www.ibm.com/support/pages/node/6213739.
- **Security Bulletin: IBM Spectrum Scale GUI is affected by weak cryptographic algorithm (CVE-2020-4350)**

  Summary:

  A security vulnerability has been identified in all levels of IBM Spectrum Scale GUI. A fix for this vulnerability is available.

  For more information, see https://www.ibm.com/support/pages/node/6214480.
- **Security Bulletin: IBM Spectrum Scale GUI is affected by verbose error message (CVE-2020-4357)**

  Summary:

  A security vulnerability has been identified in all levels of IBM Spectrum Scale GUI. A fix for this vulnerability is available.

  For more information, see https://www.ibm.com/support/pages/node/6214478.
- **Security Bulletin: IBM Spectrum Scale GUI is affected by cross-site scripting (CVE-2020-4358)**

  Summary:

  A security vulnerability has been identified in all levels of IBM Spectrum Scale GUI. A fix for this vulnerability is available.

  For more information, see https://www.ibm.com/support/pages/node/6214481.
- **Security Bulletin: IBM Spectrum Scale GUI is affected by weak crypto algorithm (CVE-2020-4349)**

  Summary:

  A security vulnerability has been identified in all levels of IBM Spectrum Scale GUI. A fix for this vulnerability is available.

  For more information, see https://www.ibm.com/support/pages/node/6214482.
- **Security Bulletin: IBM Spectrum Scale GUI is affected by weak crypto algorithm (CVE-2020-4379)**

  Summary:

  A security vulnerability has been identified in all levels of IBM Spectrum Scale GUI. A fix for this vulnerability is available.

  For more information, see https://www.ibm.com/support/pages/node/6214483.
- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale GUI where authorized user can execute unauthorized function (CVE-2020-4378)**

  Summary:

  A security vulnerability has been identified in all levels of IBM Spectrum Scale GUI. A fix for this vulnerability is available.

  For more information, see https://www.ibm.com/support/pages/node/6214484.
- **IBM Spectrum Scale Erasure Code Edition (ECE) Alert: Potential data corruption with NVMe drive.**

  Abstract:

  IBM has identified a potential data corruption issue in IBM Spectrum Scale Erasure Code Edition (ECE) with NVMe drive while having network issue.

  For more information, see https://www.ibm.com/support/pages/node/6210439.
- **IBM Spectrum Scale(GPFS) Alert for V4.2 and V5.0 levels: possible silent data corruption may happen on snapshot files.**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale (GPFS) V4.2.0.0 through 4.2.3.19 (ESS 4.0 through ESS 5.2.8), and V5.0.0.0 through 5.0.4.2 (ESS 5.3 through ESS 5.3.5.1)levels, in which undetected data loss or corruption may result from incorrect data being read from snapshot files, after a snapshot deletion or while operations involving data copy-on-write to latest snapshot files are in progress.

  For more information, see https://www.ibm.com/support/pages/node/6213729.
- **IBM Spectrum Scale (GPFS) Alert : Versions prior to 5.0.4.2 (ESS 5.3.5.1 and ESS 6.0.0.1) are affected by an issue in offline fsck which may result in metadata or data loss.**

Abstract:

IBM has identified an issue in IBM Spectrum Scale (GPFS), versions prior to 5.0.4.2, in which offline fsck may fail to report and repair duplicate reference corruption present in the inode 0 files of an active file system and snapshots of that file system, resulting in loss of data or metadata or undetected data corruption.Refer to the "GPFS architecture" section in the "Concepts, Planning, and Installation Guide" for a description of inode 0 file a.k.a inode file.

- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale where an unprivileged user to cause denial of service in kernel (CVE-2020-4411)**

  Summary:

  A security vulnerability has been identified in all levels of IBM Spectrum Scale that could allow a local attacker to cause a denial of service. A fix for this vulnerability is available.

  For more information, see https://www.ibm.com/support/pages/node/6209002.
- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale where an unprivileged user to cause denial of service(CVE-2020-4412)**

  Summary:

  A security vulnerability has been identified in all levels of IBM Spectrum Scale that could allow a local attacker to cause a denial of service. A fix for this vulnerability is available.

  For more information, see https://www.ibm.com/support/pages/node/6209004.
- **IBM Spectrum Scale (GPFS) Alert : Multiple NFS-Ganesha issues may end up using freed memory leading to a crash or a hang.**

  Abstract:

  NFS-Ganesha shipped in IBM Spectrum Scale V5.0.4.0 to V5.0.4.3 may end up using freed memory leading to a crash or a hang while trying to re-use in-memory chunking data structure as part of executing a directory listing (NFS READDIR) request.

  For more information, see https://www.ibm.com/support/pages/node/6207920.
- **Security Bulletin: A vulnerability in IBM WebSphere® Application Server affects IBM Spectrum Scale**

  Summary:

  There is a vulnerability in IBM WebSphere Application Server, used by IBM Spectrum Scale, which could allow a remote attacker to cause a denial of service.

  For more information, see https://www.ibm.com/support/pages/node/6192879.
- **IBM Spectrum Scale(GPFS) Alert for V4.2 and V5.0 levels: data corruption may happen on compressed files.**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale (GPFS) V4.2.0.0 through 4.2.3.20 (ESS 4.0 through 5.2.9), and V5.0.0.0 through 5.0.4.2 (ESS 5.3 through 5.3.5.1) levels, in which the concurrent use of mmap write and compression operations may cause the data in data blocks being compressed to be corrupted.

  For more information, see https://www.ibm.com/support/pages/node/5736753.
- **IBM Spectrum Scale (GPFS) Alert: Releases 4.2.3.18 or later and 5.0.4.0 or later have issues resulting in kernel crashes on RHEL7.7 with kernel 3.10.0-1062.18.1 or higher.**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale (GPFS) versions that support RHEL 7.7 (4.2.3.18 or later and 5.0.4.0 or later) in which a RHEL 7.7 node running kernel versions 3.10.0-1062.18.1 or higher might encounter a kernel crash while performing operations on files in the file system.

  For more information, see https://www.ibm.com/support/pages/node/6193107.
- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale where an unprivileged user could execute commands as root (CVE-2020-4273)**

  Summary:

  A security vulnerability has been identified in all levels of IBM Spectrum Scale that could allow an underprivileged attacker to execute commands as root. A fix for this vulnerability is available.

  For more information, see https://www.ibm.com/support/pages/node/6151701.
- **IBM Spectrum Scale (GPFS) 4.2.3 (ESS 5.2) and 5.0 (ESS 5.3) levels Alert: command "mmchdisk start" may succeed without synchronizing the replicas and may result in undetected data corruption.**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale (GPFS) V4.2.0.0 through V4.2.3.18 (ESS 4.0 through ESS 5.2.8) and V5.0.0.0 through V5.0.4.1 (ESS 5.3 through ESS 5.3.5) in which, in a replicated file system, the command `mmchdisk <file system> start` might indicate success even without being able to synchronize all the replicas. That might result in undetected data corruption, as attempts to read files might retrieve data from an out-of-date or uninitialized replica. One known scenario where the command is unable to synchronize all the replicas but still indicates success happens in an encrypted file system, when problems occur in accessing the key servers while the command is being processed.

For more information, see https://www.ibm.com/support/pages/node/3555453.

- **Security Bulletin: A vulnerability in Samba affects IBM Spectrum Scale SMB protocol access method (CVE-2019-14907)**

  Summary:

  A Samba vulnerability affects IBM Spectrum Scale SMB protocol access method that could cause denial of service. A fix for this vulnerability is available.

  For more information, see https://www.ibm.com/support/pages/node/5693486.

- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale where an attacker can cause a denial of service (CVE-2020-4217)**

  Summary:

  A security vulnerability has been identified in all levels of IBM Spectrum Scale that could allow an attacker to cause a denial of service. A fix for this vulnerability is available.

  For more information, see https://www.ibm.com/support/pages/node/5693463.

- **IBM Spectrum Scale (GPFS) 5.0.4 levels: possible metadata or data corruption during file system log recovery**

  Abstract:

  IBM has identified a problem with the IBM Spectrum Scale parallel log recovery function at V5.0.4.0 - V5.0.4.1, which might result in metadata corruption or undetected data corruption during the course of a file system recovery.

  For more information, see https://www.ibm.com/support/pages/node/1274428.

- **IBM Spectrum Scale Active File Management (AFM) issues which may result in undetected data corruption.**

  Abstract:

  IBM has identified issues affecting Active File Management (AFM) in IBM Spectrum Scale V5.0.0.0 through V5.0.4.1, which might result in undetected data corruption.

  For more information, see https://www.ibm.com/support/pages/node/1172272.

- **IBM Spectrum Scale (GPFS): Avoid using mmrestripefs -c to repair replicas.**

  Abstract:

  IBM recommends that users not invoke the command `mmrestripefs -c` to compare and fix data and metadata replicas, as in some cases this might result in copying bad replica data to formerly good replicas.

  For more information, see https://www.ibm.com/support/pages/node/1114845.

- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale where remote authenticated attacker can execute arbitrary command(CVE 2019-4715)**

  Summary:

  A security vulnerability has been identified in all levels of IBM Spectrum Scale that could allow remote authenticated attacker to execute arbitrary command on the system. This vulnerability only affects systems where the SMB protocol is enabled. A fix for this vulnerability is available.

  For more information, see https://www.ibm.com/support/pages/node/1118913.

- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale which allows users to embed arbitrary JavaScript code in the Web UI (CVE-2019-4665)**

  Summary:

  A security vulnerability has been identified in all levels of IBM Spectrum Scale that could allow users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. A fix for this vulnerability is available.

  For more information, see https://www.ibm.com/support/pages/node/1118937.

- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale where local attacker can execute arbitrary commands on the system (CVE-2019-4664)**

  Summary:

  IBM Spectrum Scale could allow local attacker to execute specially crafted request for an exploitation of the system. Fix is available for this vulnerability.

  For more information, see https://www.ibm.com/support/pages/node/1127727.

- **Security Bulletin: A vulnerability in Samba affects IBM Spectrum Scale SMB protocol access method (CVE-2019-10197)**

Summary:

A Samba vulnerability affects IBM Spectrum Scale SMB protocol access method that could allow a remote attacker to bypass security restrictions and gain access to the contents of directories outside of the share.

For more information, see https://www.ibm.com/support/pages/node/1086687.

- **IBM Spectrum Scale (GPFS) V5.0.3.0 through 5.0.4.0: During upgrade from release level 5.0.3.x to 5.0.4.0 with clustered watches enabled may result in loss of file system events.**

  Problem:

  When upgrading from V5.0.3.x to 5.0.4 with **clustered watches enabled**, users might see a watch go into the Auto Disabled state during the upgrade (this can be seen with the `mmwatch all status` command). If this happens, the events generated on the file system at that time have been lost and cannot be recovered.

  For more information, see https://www.ibm.com/support/pages/node/1074624.

- **IBM Spectrum Scale (GPFS) : Versions prior to 4.2.3.18 and 5.0.4.0 are affected by an issue in online fsck which may result in metadata or data loss.**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale (GPFS) versions prior to 4.2.3.18 and 5.0.4.0, in which online fsck might report false positive and incorrectly report such lost blocks might result in loss of data or metadata or undetected data corruption.

  For more information, see https://www.ibm.com/support/pages/node/1074228.

- **Flashes (Alerts): IBM Spectrum Scale (GPFS) 4.2.3 and 5.0 levels: concurrent mmap and read from the same files may result in undetected data corruption**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale (GPFS) V4.2.3.15 through 4.2.3.16, and V5.0.3.0 through 5.0.3.2 levels, in which concurrent read and mmap operations on the same file by multiple processes or threads might result in undetected data corruption in the form of a read operation returning incorrect data.

  For more information, see the complete bulletin at https://www-01.ibm.com/support/docview.wss?uid=ibm10960396.

- **Security Bulletin: A vulnerability in IBM WebSphere Application Server affects IBM Spectrum Scale (CVE-2019-4046)**

  Summary:

  There is a vulnerability in IBM WebSphere Application Server, which is used by IBM Spectrum Scale. This issue allows a remote attacker to cause a denial of service condition.

  For more information, see the complete bulletin at https://www-01.ibm.com/support/docview.wss?uid=ibm10957743.

- **Flashes (Alerts): IBM Spectrum Scale (GPFS): Releases 4.2.3.13 or later and 5.0.2.2 or later have issues where kernel crashes on RHEL7.6**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale (GPFS) versions that support RHEL 7.6 (4.2.3.13 or later and 5.0.2.2 or later) in which a RHEL 7.6 node running kernel versions 3.10.0-957.19.1 or higher, including 3.10.0-957.21.2, might encounter a kernel crash while running I/O operations. A fix is available.

  For more information, see the complete bulletin at https://www-01.ibm.com/support/docview.wss?uid=ibm10887729.

- **Flashes (Alerts): IBM Spectrum Scale (GPFS): Releases 4.2.3.13 or later and 5.0.2.2 or later have issues where kernel crashes on RHEL7.6**

  Summary:

  IBM has identified an issue in IBM Spectrum Scale (GPFS) versions that support RHEL7.6 (4.2.3.13 or later and 5.0.2.2 or later), in which a RHEL7.6 node running kernel versions 3.10.0-957.19.1 or higher, including 3.10.0-957.21.2, might encounter a kernel crash while running an IO operations.

  For more information, see the complete bulletin at https://www-01.ibm.com/support/docview.wss?uid=ibm10887213.

- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale with CES stack enabled that could allow sensitive data to be included with service snaps. This data could be sent to IBM during service engagements (CVE-2019-4259)**

  Summary:

  A security vulnerability has been identified in IBM Spectrum Scale with CES stack enabled that could allow sensitive data to be included with service snaps. This data could be sent to IBM during service engagements (CVE-2019-4259).

  For more information, see the complete bulletin at https://www-01.ibm.com/support/docview.wss?uid=ibm10883568.

- **Security Bulletin: A vulnerability in IBM WebSphere Application Server affects IBM Spectrum Scale (CVE-2018-10237)**

  Summary:

There is a vulnerability in IBM WebSphere Application Server, which is used by IBM Spectrum Scale. This issue allows a remote attacker to cause a denial of service condition.

For more information, see the complete bulletin at https://www-01.ibm.com/support/docview.wss?uid=ibm10878268.

- **Flashes (Alerts): IBM Spectrum Scale (GPFS) running CES NFS service: possible undetected data corruption with NFS client using CES-based NFS service to store data**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale when running CES-based NFS (a.k.a NFS Ganesha server) services in which an application running on an NFS client might experience undetected data corruption. If the NFS Ganesha server starts file sync for processing a data commit request from NFS client and, at the same time, there is a "stripe group panic," or the mmfsd deamon is killed on the NFS Ganesha server, then data that was supposed to have been written to disk might be lost.

  For more information, see the complete bulletin at http://www.ibm.com/support/docview.wss?uid=ibm10875558.
- **Security Bulletin: A vulnerability in IBM WebSphere Application Server affects IBM Spectrum Scale (CVE-2018-1901)**

  Summary:

  There is a vulnerability in the IBM WebSphere Application Server, which is used by IBM Spectrum Scale. This issue could allow a remote attacker to temporarily gain elevated privileges on the system.

  For more information, see the complete bulletin at https://www-01.ibm.com/support/docview.wss?uid=ibm10871590.
- **Flashes (Alerts): IBM Spectrum Scale (GPFS) V5.0.0.0 through 5.0.2.1 running CES NFS service: NFSv4 client application opening a file with the O_TRUNC option may result in undetected data corruption on opening the same file again**

  Abstract:

  IBM has identified an issue in IBM Spectrum Scale V5.0.0.0 through V5.0.2.1 when running CES-based NFS (also known as NFS Ganesha server) services in which an application running on an NFSv4 client might experience a data loss. If the application opens a file with the O_TRUNC option, then modifies (write/append) it, and then again opens (without the O_TRUNC option) the same file (without first closing it), then the file will be truncated, leading to undetected data corruption.

  For more information, see the complete bulletin at http://www.ibm.com/support/docview.wss?uid=ibm10871896.
- **Flash (Alerts): IBM Spectrum Scale (GPFS) V4.1.1.0 through 5.0.1.1: a read from or write to a DMAPI-migrated file may result in undetected data corruption or a recall failure**

  Abstract:

  IBM has identified a problem in IBM Spectrum Scale V4.1.1.0 through 5.0.1.1 in which under some conditions reading a DMAPI-migrated file might return zeroes instead of the actual data. Furthermore, a DMAPI-migrate operation or writing to a DMAPI-migrated file might cause the size of the stub file to be updated incorrectly, which might cause a mismatch between the file size recorded in the stub file and in the migrated object. This might result in failure of a manual or transparent recall when triggered by a subsequent read from or write to the file.

  For more information, see the complete bulletin at http://www.ibm.com/support/docview.wss?uid=ibm10741243.
- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale where the use of Local Read Only Cache (LROC) may result in directory corruption and undetected data corruption in regular files.**

  Summary:

  After cached data is moved from memory to the LROC device, any changes to that data should trigger invalidation of the data stored in LROC. Due to a problem with invalidation logic, it is possible for invalidation of this LROC data to be skipped. This could lead to stale or incorrect data to be recalled from LROC and data in memory to become corrupted, with potential for the data on disks to also become corrupted.

  For more information, see the complete bulletin at https://www.ibm.com/support/docview.wss?uid=ibm10793719.
- **Flash (Alerts): IBM has identified a problem in IBM Spectrum Scale (GPFS) V4.1.0 thru V5.0.2 levels where the use of Local Read Only Cache (LROC) may result in directory corruption or undetected data corruption in regular files**

  Summary:

  After cached data is moved from memory to the LROC device, any changes to that data should trigger invalidation of the data stored in LROC. Due to a problem with the invalidation logic, it is possible for invalidation of this LROC data to be skipped. This may lead to stale or incorrect data being recalled from LROC and data in memory becoming corrupted, with potential undetected data corruption on disk.

  For more information, see the complete bulletin at http://www.ibm.com/support/docview.wss?uid=ibm10741439.
- **Security Bulletin: A vulnerability in IBM WebSphere Application Server affects IBM Spectrum Scale**

  Summary:

  There is a vulnerability in the IBM WebSphere Application Server, which is used by IBM Spectrum Scale. This issue allows a remote attacker to conduct a man-in-the-middle attack.

  For more information, see the complete bulletin at https://www-01.ibm.com/support/docview.wss?uid=ibm10742215.

- **Security Bulletin: A vulnerability in IBM Java SDK affects IBM Spectrum Scale**

  Summary:

  There is a vulnerability in IBM SDK Java Technology Edition, Version 8 used by IBM Spectrum Scale. This issue was disclosed as part of the IBM Java SDK updates in July 2018.

  For more information, see the complete bulletin at https://www-01.ibm.com/support/docview.wss?uid=ibm10735169.
- **Security Bulletin: A vulnerability in Samba affects IBM Spectrum Scale SMB protocol access method (CVE-2018-10858)**

  Summary:

  A Samba vulnerability affects IBM Spectrum Scale SMB protocol access method to a heap-based buffer overflow, caused by improper bounds checking by libsmbclient. By sending an overly long file name, a remote attacker could overflow a buffer and execute arbitrary code on the system or cause the application to crash.

  For more information, see the complete bulletin at https://www-01.ibm.com/support/docview.wss?uid=ibm10732876.
- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale that could allow a unprivileged, auntheticated user to read aribiratry file on node**

  Summary:

  IBM Spectrum Scale could allow an unprivileged, authenticated user with access to a GPFS node to read arbitrary files available on this node.

  For more information, see the complete bulletin at https://www-01.ibm.com/support/docview.wss?uid=ibm10732713.
- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale that could allow an unprivileged, authenticated user to forcefully unterminate and deny access to data available through GPFS**

  Summary:

  IBM Spectrum Scale could allow an unprivileged, authenticated user with access to a GPFS node to forcefully terminate GPFS and deny access to data available through GPFS.

  For more information, see the complete bulletin at https://www-01.ibm.com/support/docview.wss?uid=ibm10732717.
- **Technote (Troubleshooting): IBM Spectrum Scale: Vormetric DSM V6.0.2, V6.0.3 and V6.1.x releases are not supported with IBM Spectrum Scale Encryption**

  Problem:

  Vormetric DSM V6.0.2, V6.0.3, and V6.1.x user interface do not support creation of KMIP objects such as the Master Encryption Keys (MEKs) used by IBM Spectrum Scale encryption, and as a result, IBM Spectrum Scale encryption cannot use these DSM releases.

  For more information, see the complete technote at https://www-01.ibm.com/support/docview.wss?uid=ibm10734479.
- **Technote (Troubleshooting): IBM Spectrum Scale: remotely mounted file system panic on accessing cluster after upgrading the owning cluster first**

  Problem:

  When running a remotely mounted cluster environment (multi-cluster with remotely mounted file systems) and the owning cluster and accessing cluster are at 5.0.0.x or 5.0.1.x code level with file audit logging enabled, and the owning cluster is upgraded first to 5.0.2.x, and `mmchconfig --release=`LATEST is run, then the remotely mounted file systems on the accessing clusters will panic and not be able to mount.

  For more information, see the complete technote at https://www-01.ibm.com/support/docview.wss?uid=ibm10734629.
- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale that could allow a local, unprivileged user to cause a kernel panic (CVE-2018-1782)**

  Summary:

  IBM Spectrum Scale could allow a local, unprivileged user to cause a kernel panic on a node running IBM Spectrum Scale by accessing a file that is stored on an IBM Spectrum Scale file system with `mmap`, or by executing a crafted file stored on an IBM Spectrum Scale file system.

  For more information, see the complete bulletin at https://www-01.ibm.com/support/docview.wss?uid=ibm10730967.
- **Flashes (Alerts): IBM Spectrum Scale (GPFS) V4.2 and 5.0.0 levels, Linux only: combined usage of compression and Local Read Only Cache (LROC) may result in undetected data corruption in regular files**

  Abstract:

  In the process of either decompressing or truncating compressed files, some data blocks might be deallocated. A problem has been identified in which the data might be recalled from LROC devices if the data for these deallocated blocks was stored into LROC devices before deallocation. As a result of the data being recalled from the LROC devices, data in memory might become corrupted, with potential for the data on disks to also become corrupted.

Note: Many types of file modifications (e.g., write, punch hole) of the data of compressed files could trigger an on-the-fly transparent uncompression operation, including GPFS's command line or policy interfaces (e.g., `mmrestripefs -z`, `mmchattr --compression no`).

For more information, see the complete flash at http://www-01.ibm.com/support/docview.wss?uid=ibm10713659.

- **Flashes (Alerts): IBM Spectrum Scale Active File Management (AFM) and AFM Asynchronous Disaster Recovery (ADR) issues, which may result in undetected data corruption**

  Abstract:

  IBM has identified certain issues affecting Active File Management (AFM) and AFM Asynchronous Disaster Recovery (ADR) in IBM Spectrum Scale, which might result in undetected data corruption.

  1. AFM might intermittently read files from the home cluster incorrectly if the replication factor is more than one at the cache cluster, which might result in undetected data corruption.
  2. AFM cache might incorrectly read an HSM migrated file from the home cluster due to the incorrect calculation of the file sparseness information, which could potentially result in undetected data corruption.
  3. AFM `mmafmctl Device resync/failover` and AFM ADR `mmafmctl Device changeSecondary` commands might miss copying data to the home or secondary cluster (from the other cluster) when the in-memory queue is dropped with pending in-place writes.
  4. AFM Asynchronous Disaster Recovery (ADR) could cause some files to be missing from the RPO snapshot at the secondary if recovery was run from the recovery+RPO snapshot.
  5. AFM might not replicate the data when the `dm_write_invis()` API is used to write. In addition, the `dm_read_invis()` API might read incorrect data if the file is not already cached.

  For more information, see the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ibm10713675.

- **IBM Spectrum Scale Software/IBM Elastic Storage Server: Release Recommendation**

  Abstract:

  IBM Spectrum Scale customers running prior versions are encouraged to upgrade to V4.2.3.8 in order to benefit from numerous quality improvement fixes included in this release. IBM Elastic Storage Server (ESS) V5.2.2.1 also leverages IBM Spectrum Scale V4.2.3.8 to provide additional robustness and reliability. IBM also strongly recommends that ESS systems running prior versions be upgraded to ESS 5.2.2.1 or later releases.

  For more information, see the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1012386.

- **Technote (troubleshooting): The pre-built SELinux policy within RHEL7.x conflicts with IBM Spectrum Scale NFS Ganesha**

  Problem (Abstract):

  Ganesha running on CES nodes with SELinux in enforcing mode and selinux-policy-targeted-3.13.x and later installed causes the start of Ganesha to fail and thus all CES nodes get UNHEALTHY. See https://bugzilla.redhat.com/show_bug.cgi?id=1383784.

Note: IBM Spectrum Scale does not support CES with SELinux in enforcing mode.

For more information, see the complete technote at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1009947.

- **Security Bulletin: A vulnerability in IBM Java SDK affects IBM Spectrum Scale**

  Summary:

  There is a vulnerability in IBM SDK Java Technology Edition, Version 8 used by IBM Spectrum Scale. This issue was disclosed as part of the IBM Java SDK updates in April 2018.

  For more information, see the complete security bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1012400.

- **Security Bulletin: Vulnerabilities in GSKit affect IBM Spectrum Scale (CVE-2018-1431, CVE-2017-3736, CVE-2017-3732, CVE-2016-0705)**

  Summary:

  Vulnerabilities in GSKit affect IBM Spectrum Scale where:

  - A local attacker could obtain control of the IBM Spectrum Scale daemon to access and modify files in the IBM Spectrum Scale file system, and possibly to obtain administrator privileges on the node (CVE-2018-1431).
  - OpenSSL could allow a remote attacker to obtain sensitive information, which is caused by a carry propagation flaw in the x86_64 Montgomery squaring function `bn_sqrx8x_internal()`. An attacker with online access to a system that is not patched could exploit this vulnerability to obtain information about the private key (CVE-2017-3736).
  - OpenSSL could allow a remote attacker to obtain sensitive information, which is caused by a carry propagating bug in the x86_64 Montgomery squaring procedure. An attacker could exploit this vulnerability to obtain information about the private key (CVE-2017-3732).
  - OpenSSL is vulnerable to a denial of service, which is caused by a double-free error when parsing DSA private keys. An attacker could exploit this vulnerability to corrupt memory and cause a denial of service (CVE-2016-0705).

  For more information, see the complete security bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1012049.

- **Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale with CES stack enabled that could allow sensitive data to be included with service snaps. This data could be sent to IBM during service engagements (CVE-2018-1512)**

  Summary:

  A security vulnerability has been identified in IBM Spectrum Scale with CES stack enabled that could allow sensitive data to be included with service snaps. This data could be sent to IBM during service engagements (CVE-2018-1512).

  For more information, see the complete security bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1012325.
- **Security Bulletin: Vulnerabilities in Samba affect IBM Spectrum Scale SMB protocol access method (CVE-2017-14746, CVE-2017-15275)**

  Summary:

  Vulnerabilities in Samba affect IBM Spectrum Scale SMB protocol access method in a manner that could result in the following issues:

  – Allowing a remote attacker to execute arbitrary code on the system, caused by a use-after-free memory error (CVE-2017-14746).
  – Allowing a remote attacker to obtain sensitive information, caused by a heap memory information leak (CVE-2017-15275).

  For more information, see the complete security bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1012067.
- **Flash (Alert): IBM Spectrum Scale (GPFS): Undetected corruption of archived sparse files (Linux)**

  Abstract:

  IBM has identified an issue with IBM GPFS and IBM Spectrum Scale for Linux environments in which a sparse file may be silently corrupted during archival, which could result in the file being restored incorrectly.

  For more information, see the complete flash at http://www.ibm.com/support/docview.wss?uid=ssg1S1012054.
- **Technote (troubleshooting): IBM Spectrum Scale: Using O_DIRECT and fork(2) in the same process in Linux**

  Problem (Abstract):

  IBM Spectrum Scale: Using O_DIRECT and fork(2) in the same process in Linux.

  Symptom:

  System call read() might fail to record data into the user buffer when direct I/O is used, that is, when specifying the O_DIRECT flag when opening the file.

  For more information, see the complete technote at http://www.ibm.com/support/docview.wss?uid=ssg1S1010878.
- **Technote (troubleshooting): IBM Spectrum Scale v4.2.x may experience cluster hangs, unacceptably high CPU load spikes, or high Command Line Interface command execution time on IBM System z14**

  Problem (Abstract):

  Core components of IBM Spectrum Scale initialize and use encrypted communication. This communication is happening whenever certain IBM Spectrum Scale commands are performed, even when the system appears to be idle. Depending on the IBM System z14 configuration, cluster hangs might occur. In addition, encryption initialization might temporarily spike CPU usage to 100% and response times will slow down to unreasonable speeds.

  IBM has corrected the issues in IBM Spectrum Scale v4.2.3.6 and later releases for zLinux only.

  For more information, see the complete technote at http://www.ibm.com/support/docview.wss?uid=ssg1S1010859.
- **Security Bulletin: Vulnerabilities in Samba affect IBM Spectrum Scale SMB protocol access method (CVE-2017-12163, CVE-2017-12151, CVE-2017-12150)**

  Summary:

  Vulnerabilities in Samba affect IBM Spectrum Scale SMB protocol access method that:

  – Could allow a remote authenticated attacker to obtain sensitive information, caused by a memory leak over SMB1 (CVE-2017-12163).
  – Could provide weaker than expected security, caused by the failure to properly sign and encrypt DFS redirects when the max protocol for the original connection is set as "SMB3" (CVE-2017-12151).
  – Could allow a remote attacker to obtain sensitive information, caused by the failure to require SMB signing in SMB1/2/3 connections (CVE-2017-12150).

  For more information, see the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1010703.
- **Technote (troubleshooting): IBM Spectrum Scale support: `mmchfs -V` full command will fail on upgrade from file system 2.2**

  Problem (Abstract):

  If your file system version is still at the 2.2 level, then running `mmchfs -V` full on certain levels of IBM Spectrum Scale will cause the `mmchfs` command to fail. The file system will be unusable until the fix is applied.

  For more information, see the complete technote at http://www.ibm.com/support/docview.wss?uid=ssg1S1010654.

- **Flash (Alert): IBM Spectrum Scale: Quick restart of ctdb under SMB load can lead to a race condition**

  Abstract:

  IBM has identified an issue with IBM Spectrum Scale V4.2.0.x in which a quick restart of ctdb under SMB load can lead to a race condition that keeps ctdb stuck in an endless recovery. This can occur during upgrade or by rapidly bringing the SMB service online and offline.

  For more information, see the complete flash at http://www.ibm.com/support/docview.wss?uid=ssg1S1010618.
- **Technote (troubleshooting): IBM Spectrum Scale: SMB cluster export services (CES) must not be upgraded concurrently**

  Problem (Abstract):

  SMB cluster export services (CES) within IBM Spectrum Scale must not be upgraded concurrently nor have different versions of the `gpfs.smb` rpm active across multiple CES nodes at once.

  For more information, see the complete technote at http://www.ibm.com/support/docview.wss?uid=ssg1S1010619.
- **Flash (Alert): IBM Spectrum Scale (GPFS) AFM incorrectly replicates data when write and truncate operations are interleaved**

  Abstract:

  IBM has identified an issue with AFM in IBM GPFS (V3.5.0.0 through V3.5.0.34 or V4.1.0.0 through V4.1.0.8) and IBM Spectrum Scale (V4.1.1.0 through V4.1.1.16 or V4.2.0.0 through V4.2.3.4) levels where AFM might not transfer write operations completely when a file is truncated. This might cause a data mismatch between cache (or primary) and home (or secondary). This issue might result in undetected data corruption at home (or secondary).

  For more information, see the complete flash at http://www.ibm.com/support/docview.wss?uid=ssg1S1010629.
- **Flash (Alert): IBM Spectrum Scale NFS Cluster Export Services may experience NFSv3 access loss during upgrade from v4.2.1.x**

  Abstract:

  IBM has identified an issue with IBM Spectrum Scale v4.2.1 cluster export services (CES) that occurs during upgrades from IBM Spectrum Scale v4.2.1.x to IBM Spectrum Scale v4.2.2.0. The issue results in NFSv3 access loss if the SHORT_FILE_HANDLE option is set to True.

  For more information, see the complete flash at http://www.ibm.com/support/docview.wss?uid=ssg1S1010628.
- **Security Bulletin: IBM Spectrum Scale Object Protocols functionality is affected by a security vulnerability in Python (CVE-2017-2592)**

  Summary:

  IBM Spectrum Scale Object Protocols functionality is affected by a security vulnerability in Python that could allow a local authenticated attacker to obtain sensitive information, which is caused by including sensitive data in the *CatchError* class. A local attacker could exploit this vulnerability to obtain sensitive information.

  For more information, see the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1010471.
- **Flash (Alert): IBM Spectrum Scale v4.2.3.1 and v4.2.3.2 installation toolkit on ppc64 platform(/usr/lpp/mmfs/4.2.3.x/installer/spectrumscale) might fail when attempting to run ./spectrumscale install, deploy, or upgrade**

  Abstract:

  IBM has identified an issue with IBM Spectrum Scale v4.2.3.1 and v4.2.3.2 of the installation toolkit on ppc64 in which the toolkit might fail if it is run multiple times. This can occur during install, deploy, or upgrade and will give a FATAL message to the user and prevent the desired task from completing.

  For more information, see the complete flash at http://www.ibm.com/support/docview.wss?uid=ssg1S1010505.
- **Security Bulletin: A vulnerability in Samba affects IBM Spectrum Scale SMB protocol access method (CVE-2017-9461)**

  Summary:

  A Samba vulnerability affects IBM Spectrum Scale SMB protocol access method, which could allow denial of service that is caused by improper handling of dangling symlinks in smbd. A remote attacker could exploit this vulnerability to cause a `fd_open_atomic` infinite loop with high CPU usage and memory consumption on the system.

  For more information, see the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1010376.
- **Flash (Alert): IBM Spectrum Scale: AFM incorrectly replicates rename operations**

  Abstract:

  IBM has identified an issue with AFM in IBM Spectrum Scale V4.1.1.12 through V4.1.1.15 and V4.2.2.0 through V4.2.3.2 levels where AFM might incorrectly replicate the rename operations. This issue might cause undetected data loss due to some files missing at the target site.

  For more information, see the complete flash at http://www.ibm.com/support/docview.wss?uid=ssg1S1010426.
- **Flash (Alert): IBM Spectrum Scale and IBM Elastic Storage Server: Performance monitoring component potentially running fileset quota sensor on more than one node causing additional load**

Abstract:

IBM has identified a configuration issue with the performance monitoring component in IBM Spectrum Scale V4.2.2 and V4.2.3 and IBM Elastic Storage Server (ESS) 5.0 and 5.1. The default configuration is monitoring the fileset quota usage hourly from all nodes in the cluster instead of just from one node. This issue might cause more load on the system than needed and can contribute to an overload situation.

Problem Summary:

The *GPFSFilesetQuota* sensor is by default not restricted to run on a single node so that it is executed every hour from all cluster nodes. This command needs to communicate with all other nodes that have been mounted on the filesystem.

For more information, see the complete flash at http://www.ibm.com/support/docview.wss?uid=ssg1S1010423.

- **Flash (Alert): IBM Spectrum Scale (GPFS): RDMA-enabled network adapter failure on the NSD server may result in file IO error**

  Abstract:

  IBM has identified an issue with all IBM GPFS and IBM Spectrum Scale versions where the NSD server is enabled to use RDMA for file IO and the storage used in your GPFS cluster is accessed via NSD servers (not fully SAN accessible). IBM Elastic Storage Server (ESS) and GPFS Storage Server (GSS) are not affected. Under these conditions, when the RDMA-enabled network adapter fails, the issue might result in undetected data corruption for file write or read operations.

  For more information, see the complete flash at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1010233.

- **Security Bulletin: A vulnerability in Samba affects IBM Spectrum Scale SMB protocol access method (CVE-2017-2619)**

  Summary:

  A Samba vulnerability affects IBM Spectrum Scale SMB protocol access method, which could allow a remote authenticated attacker to launch a symlink attack, caused by a race condition. An attacker could exploit this vulnerability using SMB1 unix extensions or NFS to create a symbolic link from a temporary file to various files on the system, which could allow the attacker to view non-exported files.

  For more information, see the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1010155.

- **Security Bulletin: IBM Spectrum Scale Object Protocols functionality is affected by security vulnerabilities in OpenStack (CVE-2015-1852 and CVE-2015-7546)**

  Summary:

  IBM Spectrum Scale Object Protocols functionality is affected by security vulnerabilities in OpenStack that could allow:

  - A man-in-the-middle attack, caused by an error in the `api-paste.ini` configuration file. A remote attacker could exploit this vulnerability using a specially-crafted handshake to conduct man-in-the-middle attacks to decrypt and modify traffic (CVE-2015-1852)
  - A remote attacker to bypass security restrictions, caused by an error when using the PKI or PKIZ token providers. By manipulating the token contents of a revoked token, the revocation check will improperly consider the token as valid. An attacker could exploit this vulnerability using a revoked token to gain unauthorized access to cloud resources (CVE-2015-7546)

  For more information, see the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1010157.

- **Security Bulletin: A vulnerability in Samba affects IBM Spectrum Scale SMB protocol access method (CVE-2017-7494)**

  Summary:

  A Samba vulnerability affects IBM Spectrum Scale SMB protocol access method, which could allow a remote authenticated attacker to execute arbitrary code on the system. It is caused by improper access to named pipe endpoints. By uploading a specially-crafted shared library to a writeable share, an attacker could exploit this vulnerability to execute arbitrary code on the system.

  For more information, see the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1010317.

- **Flash (Alert): IBM Spectrum Scale (GPFS): Asynchronous I/O write: file size change may not be updated**

  Abstract:

  IBM has identified an issue with IBM Spectrum Scale V4.1.0.4 through V4.1.1.14 and V4.2.0.0 through V4.2.3.0 levels when asynchronous Direct I/O is used to write to a file on LINUX, using the io_submit interface.

  Problem Summary:

  As a result of an asynchronous Direct I/O write using the io_ submit interface, a file size change may not be updated correctly, which could possibly lead to undetected loss of data when a node fails before the file size change is committed to disk.

  For more information, see the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1010223.

- **Security Bulletin: Multiple vulnerabilities in IBM Java SDK affect IBM Spectrum Scale**

  Summary:

  There are multiple vulnerabilities in IBM® SDK Java™ Technology Edition, Version 8 used by IBM Spectrum Scale. These issues were disclosed as part of the IBM Java SDK updates in January 2017.

For more information, see the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1010033.

- **Flash (Alert): IBM Spectrum Scale (GPFS) V4.2.3 AFM with DMAPI-enabled file system causes mmfsd daemon failure on gateway node**

  Abstract:

  IBM identified an issue with AFM on a DMAPI-enabled filesystem in IBM Spectrum Scale V4.2.3 where health monitoring is enabled by default, which causes an `mmfsd` daemon assert on the gateway node. This issue might cause the `mmfsd` daemon on the gateway nodes to fail and restart repeatedly.

  For more information, see the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1010103.

- **Technote: IBM Spectrum Scale support: Kernel crashes on Ubuntu 16.04.1 with kernel version 4.4.0-57 or later**

  Summary:

  When using Ubuntu 16.04.1 and upgrading the kernel version to 4.4.0-57 or later, you might encounter a kernel crash issue when there are some operations involving setting and removing an extended file attribute (for example, using the `setxattr` and `removexattr` syscall).

  For more information, see the complete technote at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1010071.

- **Security Bulletin: Vulnerabilities in Samba affect IBM Spectrum Scale SMB protocol access method (CVE-2016-2126, 2016-2125)**

  Summary:

  Samba vulnerabilities affect IBM Spectrum Scale SMB protocol access method, which could allow the following events to occur:

  – A remote authenticated attacker to gain elevated privileges on the system, caused by forwarding a Ticket Granting Ticket (TGT) to other service when using Kerberos authentication. An attacker could exploit this vulnerability to impersonate the authenticated user and gain elevated privileges on the system (2016-2125).
  – A remote authenticated attacker to gain elevated privileges on the system, caused by the failure of handling the PAC checksum. By using a specially-crafted Kerberos ticket, an authenticated attacker could exploit this vulnerability to gain privileges or cause the winbind process to crash (2016-2126).

  See the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1009714.

- **Technote: IBM Spectrum Scale support: 'blk_cloned_rq_check_limits: over max size limit' errors**

  Abstract:

  If you are using a GPFS block size larger than 512 Kbytes, you may encounter 'blk_cloned_rq_check_limits: over max size limit' errors, which lead to dm-multipath path failure. GPFS then will not be able to access the underlying block device.

  See the complete technote at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1009622.

- **Security Bulletin: IBM Spectrum Scale Object Protocols functionality (Linux Standard and Advanced) is affected by security vulnerabilities in the TLS and SSL protocols (CVE-2015-2808 and CVE-2014-3566)**

  Summary:

  The IBM Spectrum Scale object protocols functionality on the Linux (standard and advanced) platform is affected by security vulnerabilities in the TLS and SSL protocols.

  See the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1009336

  .

- **Flash (Alert): IBM Spectrum Scale Active File Management (AFM) and AFM Asynchronous Disaster Recovery (DR)**

  Abstract:

  IBM has identified certain situations with respect to Active File Management (AFM) and AFM Asynchronous Disaster Recovery (DR) in IBM Spectrum Scale that may result in undetected data corruption:

  – AFM may intermittently read files from the home cluster incorrectly which could result in undetected data corruption due to Direct IO usage.
  – AFM may have undetected data corruption when eviction and read operations run in parallel on the same file.
  – AFM cache may incorrectly read a file from the home cluster due to the incorrect calculation of the file sparseness information, potentially resulting in undetected data corruption.
  – If parallel IO is enabled, AFM and AFM Asynchronous DR may experience undetected data corruption with failover, resync and changeSecondary commands.
  – AFM Asynchronous DR failback may read HSM migrated files from the acting AFM Primary cluster (originally the AFM Secondary cluster) as sparse files, potentially resulting in the AFM cache to return incorrect data (all zeros) to an application on a read.

  See the complete bulletin at either http://www-01.ibm.com/support/docview.wss?uid=ssg1S1009244 or http://www-01.ibm.com/support/docview.wss?uid=isg3T1024249.

- **Flash (Alert): IBM Spectrum Scale Installation Toolkit**

Abstract:

IBM Spectrum Scale installation toolkit may fail due to a package conflict if EPEL repos are enabled

Problem Summary:

You must disable all configured EPEL repositories on all nodes added in the spectrumscale installation toolkit before proceeding with an install, deploy, or upgrade.

See the Flash at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1009275

- **Flash (Alert): IBM Spectrum Scale (GPFS) V4 Asynchronous I/O write**

  Abstract:

  IBM has identified an issue with IBM Spectrum Scale V4.1.0.4 through V4.1.1.7 and V4.2.0.0 through V4.2.0.3 levels when asynchronous Direct I/O is used to write to a file on LINUX, using the io_submit interface.

  Problem Summary:

  As a result of an asynchronous Direct I/O write using the io_ submit interface, a user file may contain undetected data corruption via writing of stale data to disk.

  See the complete bulletin at either http://www-01.ibm.com/support/docview.wss?uid=ssg1S1007917 or http://www.ibm.com/support/docview.wss?uid=isg3T1023951

- **Security Bulletin: Vulnerabilities in OpenStack affect IBM Spectrum Scale V4.2 and V4.1.1 (CVE-2015-8466 and CVE-2016-0738)**

  Summary:

  OpenStack vulnerabilities that could allow: - with OpenStack Swift 3, a remote attacker to launch a replay attack affects IBM Spectrum Scale (CVE-2015-8466) - with OpenStack Object storage(Swift), a remote authenticated attacker could exploit this vulnerability to consume all available proxy-server resources (CVE-2016-0738)

  See the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1005833

- **Flash (Alert): IBM Spectrum Scale (GPFS) V4.2 and V4.1.1 AFM Async DR requirement for planning**

  Abstract:

  Our initial feedback from the field suggests that success of a disaster recovery solution depends on administration discipline, including careful design, configuration and testing. Considering this, IBM has decided to disable the Active File Management- based Asynchronous Disaster Recovery feature (AFM DR) by default and require that customers deploying the AFM DR feature first review their deployments with IBM Spectrum Scale development. You should contact Spectrum Scale Support at scale@us.ibm.com to have your use case reviewed. IBM will help optimize your tuning parameters and enable the feature. Please include this message while contacting IBM Support.

  See the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1005817

- **Flash (Alert): IBM Spectrum Scale (GPFS) V4.2 AFM cache reads an HSM migrated file from home as a sparse file**

  Summary:

  IBM has identified an issue with AFM in IBM Spectrum Scale V4.2.0.0 through 4.2.0.2 levels when the AFM cache reads the HSM migrated files from home (running IBM Spectrum Scale V4.2 or later) as a sparse file. This issue may cause the cache to have undetected data corruption and may return incorrect data (all zeros) to an application on read.

  See the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1005766

- **Security Bulletin: IBM Spectrum Scale, with the Spectrum Scale GUI installed, is affected by a security vulnerability (CVE-2016-0361)**

  Summary:

  A security vulnerability has been identified in the current levels of IBM Spectrum Scale V4.2.0.0 thru V4.2.0.1, with the Spectrum Scale GUI installed, that could allow a remote unprivileged user to obtain sensitive information including ADMIN passwords used to access other components of the system.

  See the complete bulletin at http://www.ibm.com/support/docview.wss?uid=ssg1S1005742

- **Security Bulletin: Vulnerability in Samba affects IBM Spectrum Scale SMB protocol access method (CVE-2016-2119)**

  Summary:

  A Samba vulnerability which could allow a remote attacker to conduct spoofing attacks affects IBM Spectrum Scale SMB protocol access method.

  See the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1009255

- **Security Bulletin: Multiple vulnerabilities in Samba – including Badlock - affect IBM Spectrum Scale SMB protocol access method**

  Summary:

Samba vulnerabilities were disclosed on April 12, 2016. Samba is used by IBM Spectrum Scale SMB protocol access method. IBM Spectrum Scale has addressed the applicable CVEs including the vulnerability commonly referred to as “Badlock”.

See the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1005740

- **Security Bulletin: IBM Spectrum Scale is affected by a security vulnerability (CVE-2016-0263)**

  Summary:

  A security vulnerability has been identified in the current levels of IBM Spectrum Scale V4.2, V4.1 and IBM General Parallel File System V3.5, that could allow a local user, under special circumstances, to escalate their privileges or cause a denial of service when the mmapplypolicy command is issued with certain options and syntax.

  See the complete bulletin at either http://www-01.ibm.com/support/docview.wss?uid=isg3T1023450 or http://www-01.ibm.com/support/docview.wss?uid=ssg1S1005708

- **Security Bulletin: Vulnerability in Samba affects IBM Spectrum Scale SMB protocol access method (CVE-2015-5252)**

  Summary:

  A Samba vulnerability which could allow a remote attacker to launch a symlink attack affects IBM Spectrum Scale SMB protocol access method.

  See the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1005689

- **Security Bulletin: Vulnerability in IBM Java SDK affect IBM Spectrum Scale GUI (CVE-2015-7575)**

  Summary:

  There is a vulnerability in IBM® SDK Java™ Technology Edition, Version 8 that is used by the IBM Spectrum Scale GUI.

  See the complete bulletin at http://www-01.ibm.com/support/docview.wss?uid=ssg1S1005690

- **Systemd** is replacing traditional **sysVinit** in many Linux distributions. Though **systemd** should still support traditional **sysVinit** without any changes, starting with **systemd** version 219-19, this support is not working properly, causing IBM Spectrum Scale services not to startup at boot time. If you are experiencing this problem, you can do one of the following:

  – Upgrade your nodes to IBM Spectrum Scale V4.2.0.1.

    IBM Spectrum Scale uses **systemd** to start IBM Spectrum Scale services starting with V4.2.0.1.

  – Apply the following workaround:

    ```
    rm /etc/init.d/gpfs
    cp /usr/lpp/mmfs/bin/gpfsrunlevel /etc/init.d/gpfs
    ```

  – If **systemd** is upgraded to version 219 after IBM Spectrum Scale V4.2.0.1 was already installed, you can apply the workaround in the second option or take the following step to enable IBM Spectrum Scale services to use **systemd**:

    ```
    systemctl enable /usr/lpp/mmfs/lib/systemd/gpfs.service
    ```

- **Abstract:**

  In the Advanced Edition of GPFS V4.1.0 or later, under certain circumstances, files may be incorrectly encrypted when the **AES:ECB** wrapping mode is used, possibly resulting in undetected data corruption of those files.

  Problem Summary:

  File encryption (available only in the Advanced Edition of GPFS 4.1.0 or later releases) in GPFS is controlled by encryption policy rules, which determine which files are encrypted and with what keys and algorithms. At the time an encrypted file is created, a File Encryption Key (FEK) is generated and then encrypted ("wrapped") with the Master Encryption Key (MEK), and the result is recorded as one of the file's extended attributes, along with the identity of the MEK and the encryption parameters needed to decrypt the FEK later on. The contents of the file are encrypted with the FEK being used as encryption key. A problem has been discovered in the CLiC toolkit, which is used by GPFS to perform basic encryption/decryption. The problem results in the FEK being encrypted incorrectly before getting stored as one of the file's extended attributes. The outcome is that an incorrect FEK may be produced upon opening the file. Though the file may still be read correctly on nodes of the same type as the one used when the file was created, it may be read incorrectly from other nodes. In addition, if the file is written by one of those other nodes, the file may then be retrieved incorrectly from any of the nodes, since different portions of the file may have been written using different FEKs. The problem occurs only when FIPS mode is disabled (the **FIPS1402mode** configuration variable is set to 'no') and the **AES:ECB** wrapping mode is used on a Linux x86 node with AESNI encryption acceleration. Note that **AES:ECB** is not the default wrapping mode and is not the one used if the default **DEFAULTNISTSP800131A** algorithm is configured.

  Users affected:

  Users are affected only if all of the following conditions are true:

- The file encryption capability (available only in the Advanced Edition of GPFS 4.1.0 or later releases) is used, as described in the Encryption chapter in the Advanced Administration Guide publication at http://www.ibm.com/support/knowledgecenter/STXKQY/ibmspectrumscale_welcome.html

Note: Linux on Z nodes are not affected.

- The **AES:ECB** wrapping mode is chosen when providing the encryption policy rules for a file system. Note that **AES:ECB** is not the default wrapping mode and is not the one used if the default **DEFAULTNISTSP800131A** algorithm is configured.

  The following command (and its sample output) shows the existing policy for the file system. It will clearly indicate whether the affected wrapping mode is being used:

```
mmlspolicy file system name -L

[...]

RULE 'F128' ENCRYPTION SET 'F128'
    ALGO 'AES:128:CBC:FEK:HMACSHA512'
    COMBINE 'XOR' WRAP 'AES:ECB'
    KEYS('KEY-6aaa3451-6a0c-4f2e-9f30-d443ff2ac7db:RKMKMIP3')
```

  Note that **ALGO 'DEFAULTNISTSP800131A**' is a safe setting, since it corresponds to the **AES:KWRAP** wrapping mode.

  The following command (see sample output) will show the parameters used for a given file:

```
mmlsattr -n gpfs.Encryption xyz2.enc

file name:            xyz2.enc
gpfs.Encryption:
"EAGC???N░V]0?????????????????D░░?░░;░??????????????"░_░?░46?Z? }??1?fooBar1?"
EncPar 'AES:128:CBC:FEK:HMACSHA512'
        type: wrapped FEK  WrpPar 'AES:ECB'  CmbPar 'XOR'
                KEY-6aaa3451-6a0c-4f2e-9f30-d443ff2ac7db:RKMKMIP3
```

  Note that changing the encryption policy does not affect the wrapping mode of existing files.

- The length of the file encryption key (as specified in the encryption parameter string) is set to a value longer than 128 bits (192 or 256 bits)
- The **FIPS1402mode** configuration parameter is set to **no**, which will result in the CLiC toolkit being used for encryption/decryption.

  The FIPS mode in use can be displayed with the following command:

```
mmlsconfig FIPS1402mode
```

- The cluster includes nodes which run on Linux x86 (any distro)
- At least one node in the cluster supports the AESNI instruction. The following command can be used to determine whether that CPU instruction is present:

```
grep aes /proc/cpuinfo
```

  If the command above produces some output then the AESNI instruction is present on the node.

Required Actions:

GPFS 4.1 Advanced Encryption customers should avoid use of the **AES:ECB** wrapping mode.

If the existing encryption policy rules specify **AES:ECB** then the encryption rules should be changed (with **mmchpolicy**) to use a different wrapping mode. That will ensure that files created from that point on will not use the **AES:ECB** wrapping mode.

The following applies to the users for which all the conditions under *Users affected* are true.

It is important to act promptly if your cluster may be affected by the problem (if all conditions under *Users Affected* are true). The steps described below aim to minimize the chance of any further data loss, as opposed to fixing any damage to the existing files. The existing files may or may not be recoverable (and backup copies may have been damaged as well), depending on a complex set of circumstances.

For the affected users, the following steps should be taken:

1. Run the following command and save the output. This contains the current policy rules (including any encryption rules) in place for the file system. The output should be provided to IBM Support.

   ```
   mmlspolicy file system name -L
   ```

2. The following steps above should prevent any new file from being created using **AES:ECB** as wrapping mode, and should avoid producing additional damaged files.

   a. Change the encryption policy and replace any instances of the wrapping parameter string **AES:ECB** with wrapping parameter string **AES:KWRAP**

   b. Apply the resulting policy by running

      ```
      mmchpolicy file system file containing the modified policy -I yes
      ```

3. Call IBM support as soon as possible for assistance with data recovery.

Note: In a cluster which may be affected by the problem, do not change the value of the **FIPS1402mode** variable . Changing that value (which will alter the toolkit used to encrypt/decrypt data) may cause file content to be incorrectly decrypted, since an incorrect FEK may be derived. In addition, writing to existing files -- but not reading from them -- may cause them to be damaged irreparably. For the very same reasons, also do not add nodes to the cluster which are affected by the problem differently than the original nodes in the cluster. That is, if all nodes in the cluster are affected (all nodes are Linux x86 with AESNI enabled) then do not add nodes which are not affected, or vice-versa: if the cluster is not affected then do not add nodes which are affected.

- After applying the glibc fix provided by your OS distribution for CVE-2015-0235 - GHOST: glibc gethostbyname buffer overflow (http://www.openwall.com/lists/oss-security/2015/01/27/9), a rebuild of the gpl layer is not necessary.
- **Abstract:**

  In Linux environments, GPFS may incorrectly fail writev() with EINVAL resulting in the user application failing during write.

  Problem Summary:

  IBM has identified a problem with GPFS 3.5.0.20 and GPFS 4.1.0.2 where GPFS may fail to correctly handle multiple vectors passed via the writev() system call. When a {NULL, 0} is passed as the first vector, an EINVAL error may be incorrectly returned. This would cause the user application to fail unexpectedly when writev() is called to write to a GPFS file. User data are not affected. The writev() call is most likely to have been automatically generated by the library or compiler.

  Users Affected:

  Only customers running the affected level on Linux and have applications which use the writev() system call for writes to a GPFS file. Note: The writev() call is most likely to have been automatically generated by the library or compiler. For example, using C++ stream class to write more than 1023 byte to a file will generate a writev() call that could fail with an EINVAL error.

  The following sample program shows an example for which a write using stream class may fail unexpectedly:

  ```
  #include<cassert>
  #include<cstdio>
  #include>

  int main (int argc, char** argv) {
  assert(argc == 2);

  char* data = new char[1000000];
  std::ofstream f(argv[1], std::ios_base::binary);
  f.write(data, 1023); // this would succeed
  perror("write call");
  f.flush();

  f.write(data, 1024); // this would fail
  perror("write call");
  f.flush();

  f.write(data, 1025); // this would fail
  perror("write call");
  f.flush();

  f.write(data, 1023); // this would succeed
  perror("write call");
  f.write(data, 1024); // this would succeed
  perror("write call");
  f.flush();
  ```

```
f.write(data, 1024); // this would fail
perror("write call");
f.write(data, 1023); // this would succeed
perror("write call");
f.flush();

f.write(data, 512); // this would succeed
perror("write call");
f.write(data, 512); // this would succeed
perror("write call");
f.write(data, 1024); // this would succeed
perror("write call");
f.flush();

f.close();
delete[] data;
return 0;
}
```

Recommendations:

Affected V3.5 customer should contact IBM Service for an efix containing APAR IV64863; this fix is available in GPFS 3.5.0.21(APAR IV64863) or later. V4.1 customers should upgrade to GPFS 4.1.0.3 (APAR IV64862) or later at Fix Central http://www.ibm.com/eserver/support/fixes/

- **Abstract:**

GPFS on clusters enabled for RDMA use may experience server crashes, RDMA failures, hangs, or undetected data corruption.

Problem Summary:

IBM has identified a problem with GPFS versions 3.5.0.17 efix18 and efix19, 3.5.0.19 and 4.1.0.2, for clusters enabled for GPFS RDMA when the value configured for verbsRdmasPerNode is less than the value configured for nsdMaxWorkerThreads for any NSD server. Under certain conditions, the NSD server thread may get indication that the RDMA completed successfully before the RDMA actually completes. This problem may result in NSD server crashes, RDMA failures, hung NSD server threads, or undetected data corruption.

Problem Description:

See Problem Summary.

Users Affected:

Only customers running the affected levels, configured to use RDMA, with a value of verbsRdmasPerNode that is less than the value configured for nsdMaxWorkerThreads for the NSD servers, are vulnerable to the problem.

To verify if the NSD servers are vulnerable to the problem, run the following command on each NSD server:

```
mmfsadm test verbs config | grep -e "Max RDMAs per node"
```

In the examples below:

- The value for "Max RDMAs per node max" corresponds to nsdMaxWorkerThreads.
- The value for "Max RDMAs per node curr" corresponds to verbsRdmasPerNode (which may be adjusted by GPFS).

An example of an NSD server that is not vulnerable to the problem:

In this example, "Max RDMAs per node max" reports the same value (512) as
"Max RDMAs per node curr" (512):

```
mmfsadm test verbs config | grep -e "Max RDMAs per node"
      Max RDMAs per node max             : 512
      Max RDMAs per node curr            : 512
```

An example of an NSD server that is vulnerable to the problem:

In this example, "Max RDMAs per node max" reports a value (512)
that is greater than "Max RDMAs per node curr" (128):

```
mmfsadm test verbs config | grep -e "Max RDMAs per node"
      Max RDMAs per node max             : 512
      Max RDMAs per node curr            : 128
```

Recommendations:

IBM recommends that customers vulnerable to the problem immediately install an efix including IV63698; for the affected levels, the relevant efixes are:

- If 3.5.0.17 efix18 or efix19 is installed, then install 3.5.0.17 efix20
- If 3.5.0.19 is installed, then install 3.5.0.20 or later
- If 4.1.0.2 is installed, then install 4.1.0.3 or later

Customers vulnerable to the problem but unable to immediately apply the above fix levels should run the following command to change the value of verbsRdmasPerNode to equal the value of nsdMaxWorkerThreads for each NSD Server, as a workaround. The customer may experience performance impacts while this workaround is in effect.

In this example, N = the value configured for nsdMaxWorkerThreads.

```
mmchconfig verbsRdmasPerNode=N
```

Customers vulnerable to the problem, after applying the service or workaround above, should contact GPFS support for instructions to run mmfsck to detect and repair any metadata damage.

- **Abstract:**

  A recent change in the UEFI driver update for the SAS HBA can result in damage to any disks used for GPFS which previously contained a GPT partition table (due to non-GPFS use) but are now assigned to GPFS, on upgrade.

  Content:

  The UEFI firmware includes a function for Disk GPT Table Recovery. This function will restore the GPT table from the backup GPT table which was stored at the end of the disk, and it is the default function. When a disk contains a backup GPT table but is later used as a GPFS NSD, the GPT Table Recovery action could rewrite GPFS NSD and Disk descriptor headers with the backup GPT table. Thus such NSDs will be lost after the GPT Table Recovery action.

  Recommendation:

  An **nsdcheck** script is available to run against NSD devices to determine if there is a valid backup GPT table on the device. An NSD disk is at risk if the remarks display **hasPrimaryGpt=no,hasSecondaryGpt=yes**. If the backup table is not valid, the script can then be used to clear the backup GPT table on the NSD device, prior to any firmware updates, as soon as is possible.

  Running this script is recommended for all Linux customers, as a precaution. The script when used to remove the secondary GPT will only remove it *IF AND ONLY IF* there is a GPT signature on the last sector of the NSD device but not at the beginning.

  The script is available:

  - In the samples directory with GPFS V3.4.0.29 and V3.5.0.19 from FixCentral
    - http://www-933.ibm.com/support/fixcentral/swg/selectFixes?parent=Cluster%2Bsoftware&product=ibm/power/IBM+General+Parallel+File+System&release=3.4.0&platform=All&function=all
    - http://www-933.ibm.com/support/fixcentral/swg/selectFixes?parent=Cluster%2Bsoftware&product=ibm/power/IBM+General+Parallel+File+System&release=3.5.0&platform=All&function=all
  - From the GPFS developerWorks® wiki at https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/General%20Parallel%20File%20System%20%28GPFS%29/page/GPFS%20Service%20Bulletins

Note: If you need to restore the secondary GPT signature from **GptBackupFile** to disk, contact IBM Service. This should not be done without guidance.

- NFS access to an HSM enabled GPFS file system running on levels of Linux below RHEL 6.3 and SLES 11 SP2, may hit the issue described here http://www-01.ibm.com/support/docview.wss?uid=ssg1S1004310
- Upgrading GPFS to a new major release on Linux:

  When migrating to a new major release of GPFS (for example, from GPFS 3.5 to GPFS 4.1), the supported migration path is to install the GPFS base images for the new release, then apply any required service updates. GPFS will not work correctly if you use **rpm -U** command to upgrade directly to a service level of a new major release without installing the base images first. If this should happen you must uninstall and then reinstall the **gpfs.base** package.

Advisories for Windows

Current advisories for Windows

The following IBM Spectrum Scale advisories are for Windows 10 related advisories and recommendations. These are applicable to Windows Server (2016 and later) as well:

1. User Access Control (UAC) must not be disabled on the latest Windows versions such as Windows 10. IBM Spectrum Scale now runs with UAC enabled (default OS setting).
2. The latest versions of Windows such as Windows 10 now come with a built-in anti-virus component known as Windows Defender®. While performing real-time scanning of files, Windows Defender might memory-map these files even when they are not in use by any user application. This memory-mapping of files on IBM Spectrum Scale file systems by Windows Defender in the background can result in performance degradation. Therefore, it is recommended that IBM Spectrum Scale drives and volumes be “excluded” from Windows Defender scans altogether.
3. Windows 10 version 1803 now incorporates a native Secure Shell ‘OpenSSH for Windows’. IBM Spectrum Scale requires 'OpenSSH for Cygwin', especially if the Windows node(s) join an IBM Spectrum Scale cluster that has Linux or AIX nodes. Therefore, before operating a Windows 10 node in a mixed IBM Spectrum Scale cluster, ensure that the Windows native 'OpenSSH SSH Server' is not enabled or running and that the 'Cygwin sshd' service is working reliably. Additionally, it is recommended that the Windows Subsystem for Linux (WSL) feature not be installed to avoid potential conflicts with Cygwin.

For IBM Spectrum Scale V4.1 and newer, no hotfix updates are required. It is recommended that you:

- Install the latest OS Service Pack available from Microsoft and stay current with Windows Updates.
- Cygwin should be updated periodically and stay relatively current.