October Newsletter

Subscribe/Unsubscribe

Greetings all,
I am sorry that so few of you were able to make it to TechXchange this year – overall I found it a really useful 4 days and learnt lots. It was also encouraging to see that IBM still was focused on the Power ecosystem. Please contact me if you would like to go through any of the presentations (or get copies).

A few updates to share

- TechXchange ‘24
  Overall it was a very useful event (even apart from the treatment given to all the Champions by Libby, Namitha, Kathryn and the Champion wranglers), with just enough technical sessions on Power, AIX, ESS to keep me happy.
- Had the pleasure to spend some time also with Andrey (Mr Power DevOps) and hear him talk about some of the great work he as done making AIX management and the deployment of LPARs simple, quick and repeatable (Link). Check his blog/subscribe to his newsletter for the latest updates improving deployment of Linux on Power (RHEL and SuSE) - Link
- IBM Just Published:
  IBM AIX - An executive guide to the strategy and roadmap for the IBM AIX operating system for IBM Power servers. A good overview and roadmap out to 2035
- Power11
  Is it too soon to start getting excited?…. Spyre Accelerator (MMA+); Quantum safe security; memory advances, with usual improvements in RAS, Energy optimisation.. all in 7nm!
- Power12
  It was great to get the opportunity to hear Bill Starke (IBM Power chip architect) talk about his plans for the Power chip, and the applications that he invisages it will drive.

Quick bites

Support has published “NIM Communication within a Firewall Environment”

This document covers:

- Introduction to NIM service handler or 'nimsh'
- The install process
- The clean-up process
- Protocols and the ports used by these protocols during a network install
- Breakdown of ports that need to be opened in a firewall for use with NIM
- Other firewall considerations

Link

In case you missed ….

- **PowerVM Enterprise Edition end of service reminder**

  Note that Version3.1.x (PID 5765-VE3), has the following lifecycle:

GA	09/11/2018
EOM	10/01/2025
EOS	30/04/2026

  Start planning your upgrade!

Coming soon

- **Platform enhancements:**

  IBM PowerVM VIOS 4.1.1
  IBM PowerVC for Private Cloud 2.3.0
  IBM Cloud Management Console 1.22
  IBM Power Hardware Management Console V10R3M1061

  Planned availability date

  12 December 2024, for electronic delivery
  20 December 2024, for physical delivery

  IBM PowerVM VIOS 4.1.1 includes:

  - NovaLink 2.3.0
  - Virtual Ethernet Multi Thread and Queue
  - Virtual optical device (vSCSI) backed by an NFS file
  - Virtual Fibre Channel enhanced command timing and improved performance and latency tracking
  - Enhanced device level LPM validation for storage
  - viosbr and viosupgrade command enhancements to support additional security information (such as users and groups)

  IBM PowerVC for Private Cloud 2.3.0, features include:

  - Built on OpenStack’s Caracal release
  - SLES 15 SP5, RHEL 9.4, 8.10 support
  - Live Partition Mobility (LM) across host groups
  - Security: Sudo-less access for PowerVC services
  - UI enhancements
  - Partition Placement attribute

  IBM Power Hardware Management Console appliance (HMC) and the virtual HMC (vHMC) 10.3.1061, features include:

  - Support for multiple system code updates in parallel via command line interface (CLI)
  - LPM Storage Validation new default behavior is Port + disk, with option to override the default behaviour

  IBM Cloud Management Console (CMC) 1.22.0

  - The CMC Enterprise Pools 2.0 application is enhanced to support:

  Link

- **AIX enhancements:**
  IBM AIX 7.3 TL3
  IBM AIX 7 Enterprise Edition 1.12
  IBM Private Cloud Edition 1.12
  IBM Private Cloud Edition with AIX 1.12
  and IBM PowerHA 7.2.9

  Planned availability date
  12 December 2024, for electronic delivery
  20 December 2024, for physical delivery

  IBM AIX 7.3 TL3, features include:

  - Virtual Ethernet bandwidth and transactional performance is enhanced for networking between AIX LPARs on the same physical server and across different physical servers.
  - AIX 16 MB dynamic page management has been extended to monitor and manage program text segments. This may improve the performance of very large application binaries.
  - The performance of AIX audit subsystem processing of logged events has been improved to reduce application impacts.
  - The storage key limitations with AIX Flash caching have been removed to allow for caches greater than 20 TB.
  - Fibre Channel and PCI NVMe direct attach I/O performance is improved when AIX runs with Power Firmware 1060.10 or later. Improvements can range from 20 to 60% depending on the workload details
  - The AIX nimadm utility is enhanced to support concurrent migration of multiple LPARs
  - AIX NIM is enhanced to better manage resources for multiple tenants or groups of systems from a single NIM server. This can help reduce the need to deploy and maintain multiple NIM server instances
  - AIX encrypted logical volumes and encrypted physical volume IO throughput and IO latency is improved with the exploitations of Power hardware in-core engine
  - AIX 7.3 TL3 introduces a tech preview for new infrastructure that enables live update of AIX libraries such as libc. Clients are encouraged to experiment with the new capability in non-production environments.
  - The AIX lvmstat utility is enhanced to report LVM mirror write consistency check (MWCC) statistics
  - The AIX Collection for Ansible includes the following major updates in 2024
  - AIX Toolbox for Open Source Software had a large number of new packages and existing ones updated

  IBM AIX 7 Enterprise Edition 1.12, subscription udpated to include:

  - IBM AIX 7.3 TL3 or IBM AIX 7.2 TL5
  - IBM PowerSC® 2.2
  - IBM PowerVC for Private Cloud® 2.3
  - IBM VM Recovery Manager® HA 1.8
  - IBM Tivoli® Monitoring 6.3

IBM Private Cloud Edition 1.12, this has been updated to include:

- IBM PowerSC 2.2
- IBM PowerVC for Private Cloud 2.3
- IBM VM Recovery Manager DR 1.8
- IBM Tivoli Monitoring 6.3

IBM has updated Private Cloud Edition with AIX has been updated to now include:

- IBM AIX 7.3 TL3 or IBM AIX 7.2 TL5
- IBM PowerSC 2.2
- IBM PowerVC for Private Cloud 2.3
- IBM VM Recovery Manager DR 1.8
- IBM Tivoli Monitoring 6.3

IBM PowerHA 7.2.9, features include:

- Policy Replication support for asynchronous replication
- PowerHA will tolerate and migrate along with the Live Kernel Update (LKU) and Live Library Update (LLU) update or migration process
- Encryption for non-AIX Logical Volume Manager (LVM) physical volumes such as Oracle ASM disk
- Enables failover in the event of a disk fail for Attack surface management (ASM)

Link

Redbooks and Redpapers

- **Performance and Best Practices Guide for IBM Storage FlashSystem and IBM SAN Volume Controller (for IBM Storage Virtualize 8.6)**, Redbook revised: 30 October 2024,
  Link
- **IBM Power 10 Scale Out Servers Technical Overview S1012, S1014, S1022s, S1022 and S1024**, Draft Redpaper, published: 15 October 2024,
  Link
- **IBM Power E1050 Technical Overview and Introduction**, Draft Redpaper published: 05 October 2024,
  Link
- **Using Pacemaker to Create Highly Available Linux Solutions on IBM Power**, Redbook, published: 03 October 2024
  Link

IBM alerts and notices

AIX alerts:

- **IJ52760: VETH PERFORMANCE DEGRADATION WHEN VIOS SEA IS A SENDER**

  Performance drop may be observed while sending data from SEA adapter to virtual ethernet using largesend.

  Link

- **IJ52703: LOCKING ISSUE IN VIRTUAL ADAPTER DRIVER CAUSES COMMAND AND PARTITION HANG**
  Commands hang on a virtual adapter on an NPIV client LPAR. It's possible the entire partition might suffer a hang. Issue is caused by incorrect locking in the virtual adapter driver on the client LPAR.
  Link
- **IJ52702: RENAMED LV IN IMAGE.DATA IS NOT UPDATED AFTER ALT_DISK_COPY**
  Renamed LV in a custom image.data file is not properly updated in filesystems after alt_disk_copy.
  Link
- **IJ52746: VNICSTAT NOT WORKING FOR PADMIN AFTER UPDATE**
  After updating VIOS, the vnicstat command may no longer be executable.
  ```
  $ vnicstat vnicserver0
  rksh: vnicstat: 0403-006 Execute permission denied.
  ```
  (can be fixed by correcting the command's authorisation)
  Link
- **IJ52701: BLK:FVT-DEV:FLKU:LU FAILING IN MCR PHZ AND CLVUPDATE FAIL**
  clvupdate fails to cleanup the LPAR after LiveUpdate failure
  Link
- **IJ52745: GETCONF DISKSIZE RETURNS INCORRECT LUN SIZE FOR FC-NVME DISKS**
  Environment: FC-NVMe attached FS9500 storage (physical stack).
  If LUN size is increased, bootinfo -s / getconf DISKSIZE do not show increased size value when the disks are
  opened. This caused that chvg -g does not update LVM structure accordingly.
  When disks are closed, getconf DISKSIZE provides a correct LUN size information.
  Correcting this in order to get the right LUN size correctly updated with "chvg -g" without varyoff Volume Group.
  Link
- **IJ52689: EMGR FAILS WITH AWK ERROR IF TRADEMARK SIGN IN A FILESET'S DESC**
  The emgr command will fail if a fileset's description contains a special char like the "registered trademark"
  Link
- **IJ52722: VETH PERFORMANCE DEGRADATION WHEN VIOS SEA IS A SENDER**
  Performance drop may be observed while sending data from SEA adapter to virtual ethernet using largesend.
  Link
- **IJ52688: LKU NOT USING STORAGE_TEMPLATE_OVERRIRDE**
  rootvg will not pick the template option given in storage_template_override
  Link

- **IJ52741: ALTERNATE ROOTVG OPERATIONS FAILS IN TRUSTED ENVIRONMENT**
  Operations like alt_disk_copy, alt_disk_install will fail when CHKEXEC or CHKSHLIB or CHKSCRIPT is ON and and
  STOP_UNTRUSTD or STOP_ON_CHKFAIL is ON
  Errors will be :
  - 0505-148 alt_disk_install: WARNING: an error occurred during backup.
  - /usr/bin/lslpp: Cannot run the specified program in a trusted environment.
  - Modifying ODM on cloned disk.
  - Building boot image on cloned disk.
  - /usr/sbin/bosboot: Cannot run the specified program in a trusted environment.
  - 0505-120 alt_disk_install: Error running bosboot in the cloned

  Link
- **IJ52716: AUDITPR DOES NOT SUPPORT SINGLE LINE OUTPUT FOR MULTI LINE EVENT**
  Some audit events include multiple newlines and this can cause merging of events in the audit stream.
  Link
- **Software: IJ52715: MKSECLDAP HANG**
  When running the mksecldap command, it may appear to hang. This can occur if the LDAP server being used is giving referrals, but connection attempts to the referral servers are failing and timing out.
  Link
- **IJ52837: TRUSTCHK COREDUMP WITH PTOOLS BUCKET EXEC**
  A system crash was observed.
  Link
- **IJ52825: LKU ON PVC DOES NOT REMOVE TEMP PAGING SPACE FROM CFG FILE**
  PowerVC managed Live update will not remove the temporary paging space disk stanza from the liveupdate.cf file. This leads to clvupdate reporting a failed cleanup even in a clean system.
  Link
- **IJ52823: IO FAILS ON VFC PATH, AFTER EEH ON 8GB OLDER ADAPTER**
  IO fails on VFC adapter
  Link
- **IJ52822: VIOS/AIX BOOT MAY HANG DURING BROADCOM FC HBA CONFIG**
  VIOS/AIX boot may hang while configuring the Broadcom FC HBA that has data rates equal to or more than 16Gb.
  Link

AIX Security Bulletin:

- **AIX is vulnerable to a denial of service (CVE-2024-6119) due to OpenSSL**

  Vulnerability in OpenSSL could allow a remote attacker to cause a denial of service (CVE-2024-6119). OpenSSL is used by AIX as part of AIX's secure network communications.

  Vulnerability Details

  CVE-2024-6119 - OpenSSL is vulnerable to a denial of service, caused by an error when performing certificate name checks (e.g., TLS clients checking server certificates). By sending a specially crafted request, a remote attacker could exploit this vulnerability to read an invalid memory address resulting in abnormal termination of the application process.

  Affected Products and Versions

Affected Product(s)	Version(s)
AIX	7.2
AIX	7.3
VIOS	3.1
VIOS	4.1

  The following fileset levels are vulnerable:

Fileset	Lower Level	Upper Level
openssl.base	3.0.0.0	3.0.13.1000

  Link

- **IJ52123 Potential undetected data loss can occur when copying or writing to files on an SMB share using the AIX SMB Client**

  Risk classification

  HIPER (High Impact and/or Pervasive)

  Risk categories

  Data Loss

  Affected Domain

  AIX SMB Client using oplocks and file leasing

  Abstract

  Potential undetected data loss can occur when copying or writing to files on an SMB share using the AIX SMB Client

  Description

  Potential undetected data loss can occur when copying or writing to files on an SMB share using the AIX SMB Client.

  This can only occur when oplocks and file leasing are enabled in the AIX SMB Client and the SMB server returns an asynchronous STATUS_PENDING response to the AIX SMB Client during the file copy.

  Data loss can occur even though the copy operation does not return an error.

  Recommended Action

  Update any affected smbc.rte levels in the below table.

  Alternatively, disable oplocks and file leasing for the AIX SMB Client with:

  ```
  smbctune -s smbc_oplock_enable=0 smbc_file_lease_enable=0
  ```

You can only change the value of these parameters when all SMB shares are unmounted on the AIX client system.

Affected AIX SMB Client Levels and Recommended Fixes

Minimum Affected	Maximum Affected Level	Fixing Level	Fix
smbc.rte 7.2.302.6	smbc.rte 7.2.302.5000	smbc.rte 7.2.302.5001	IJ52123
smbc.rte 7.3.302.0	smbc.rte 7.3.302.1	smbc.rte 7.3.302.2	IJ52123

Link

PowerVM Firmware alerts:

- **IBM Flexible Service Processor (FSP) has static credentials which may allow network users to gain service privileges to the FSP.**

  Vulnerability Details

  CVE-2024-45656 - IBM Flexible Service Processor (FSP) has static credentials which may allow network users to gain service privileges to the FSP.

  Affected Products and Versions

Affected Product(s)	Version(s)
Server Firmware	FW1060.00 - FW1060.10
Server Firmware	FW1050.00 - FW1050.21
Server Firmware	FW1030.00 - FW1030.61
Server Firmware	FW950.00 - FW950.C0
Server Firmware	FW860.00 – FW860.B3

  For Power10 servers, only FW1030, FW1050 and FW1060 are supported but all prior firmware releases on the listed products are vulnerable.
  For Power9 servers, only FW950 is supported but all prior firmware releases on the listed products are vulnerable.
  For Power8 servers, a mitigation is being released only for FW860 but all prior firmware releases on the listed products are vulnerable.

  Bulletin
  Link - Power8
  Link - Power9
  Link - Power10

- **Getting error HSCLA27C with rc = 69 during Live Partition Mobility**

  LPM fails with the following error;

  HSCLA27C The operation to get the physical device location for adapter UXXXX.XXX.XXXXXXX-VX-CXXX on the virtual I/O server partition XXXX has failed.

  The partition command is:

```
migmgr -f get_adapter  -t vscsi -s UXXXX.XXX.XXXXXXX-VX-CXXX -w
XXXXXXXXXXXXXXXX -W XXXXXXXXXXXXXXXX -c RPA -a
ACTIVE_LPM -d 5
```

The partition standard error is:

```
Running method '/usr/lib/methods/mig_vscsi' 69
```

Details

The error is caused when more targets than allowed are zoned to VFC adapters, causing the VIOS to receive more buffers than allowed.

*Maximum of 64 targets per virtual Fibre Channel adapter, for more up to date information, please refer to Viewing virtual Fibre Channel adapters.

Steps

Engage your local storage/switch team to verify whether the adapter in question has more targets zoned to it than allowed.

Unzone some of those targets as the VIOS is receiving more buffers than allowed, and then rezone those targets to other adapters.

Link

PowerVM Advisory:

- **Error FCA_ERR4 0x0E and FCA_ERR6 0x2B reported by FC adapters with Feature Codes EN1E/EN1F, EN1G/EN1H, EN1J/EN1K, EN2L/EN2M, or EN2N/EN2P**

Abstract

The purpose of this document is to assist with decoding the errors that may occur on Virtual I/O Server using FC adapter with Feature Code EN1E/EN1F, EN1G/EN1H, EN1J/EN1K, EN2L/EN2M, or EN2N/EN2P.

Furthermore, this document offers guidance in response to the errors.

FCA_ERR4 0x0E and FCA_ERR6 0x2B may occur in NPIV environment where

VIOS level is 3.1.4.x or 4.1.x.x

FC adapter with Feature Code/Marketing ID EN1E/EN1F, EN1G/EN1H, EN1J/EN1K, EN2L/EN2M, or EN2N/EN2P is assigned to VIOS

Link

- **Potential undetected data loss can occur on LPARs using NPIV with certain Fibre Channel adapters**

Risk classification

HIPER (High Impact and/or Pervasive)

Risk categories

Data Loss

Affected Domain

LPARs using NPIV with certain Fibre Channel adapters

Description

Potential undetected data loss can occur on LPARs using NPIV over Fibre Channel adapters with the following Feature Codes:

EN1E/EN1F, EN1G/EN1H, EN1J/EN1K, EN2L/EN2M, and EN2N/EN2P

This issue with the adapter firmware is exposed by IJ47358 in VIOS 3.1.4.4x and IJ49879 in VIOS 4.1.0.2x (or an interim fix for either APAR)

This issue can occur when the LPAR boots or when one of the LPAR targets on the SAN is removed. The port login process can cause login collisions, invalid MPIO configurations, or potentially undetected data loss.

FCA_ERR6 and FCA_ERR4 will be seen in the errpt on the VIOS if this issue occurred. More details on identifying the specific error are here.

Recommended Action

IBM is closely engaged with the adapter vendor to resolve the issue. This bulletin will be updated and another notification will be sent when a fix is available.

Until the fix is available, IBM recommends the following actions to mitigate the issue:

1. If the VIOS is running 4.1.0.20/21, apply the temporary ifix labeled 'cv41021s1a' from this link.
2. If the VIOS is running 3.1.4.40/41, apply the temporary ifix labeled 'cv31441s1a' from this link.
3. If the VIOS is running an earlier level, with an ifix installed that contains IJ47358 or IJ49879, then temporarily remove the ifix.

Please contact IBM support if any customized ifix is required for implementing the above temporary mitigations.

Link

- **VIOS 3.1.4.41**

  Notice: The following HIPER bulletin is critical to review before installing this Fix Pack to avoid potential undetected data loss for VIOS hosting NPIV connections to Fibre Channel adapters with the Feature Codes:

  EN1E/EN1F, EN1G/EN1H, EN1J/EN1K, EN2L/EN2M, and EN2N/EN2P.

  Link

  Applies to versions:

  3.1.0.0, 3.1.0.10, 3.1.0.20, 3.1.0.21, 3.1.0.30, 3.1.0.40, 3.1.0.50, 3.1.0.60, 3.1.1.0, 3.1.1.10, 3.1.1.20, 3.1.1.21, 3.1.1.25, 3.1.1.30, 3.1.1.40, 3.1.1.50, 3.1.1.60, 3.1.2.0, 3.1.2.10, 3.1.2.20, 3.1.2.21, 3.1.2.30, 3.1.2.40, 3.1.2.50, 3.1.3.0, 3.1.3.10, 3.1.3.14, 3.1.3.20, 3.1.3.21, 3.1.3.30, 3.1.4.0, 3.1.4.10, 3.1.4.20, 3.1.4.21, 3.1.4.30, 3.1.4.31, 3.1.4.40

  Link

ESS/Scale/GPFS Security Bulletin:

- **There are multiple vulnerabilities that can affect IBM Storage Scale System that are now included**

Summary

There are multiple vulnerabilities, used by IBM Storage Scale System, which could provide weaker than expected security that are now fixed.

Vulnerability Details

CVE-2024-26643 - Linux Kernel is vulnerable to a denial of service, caused by an error related to page fault dead lock on mmap-ed hwrng. A local authenticated attacker could exploit this vulnerability to cause a denial of service.

CVE-2024-27397 - Linux Kernel could allow a local authenticated attacker to gain elevated privileges on the system, caused by a use-after-free flaw in the netfilter subsystem. By sending a specially crafted request, an authenticated attacker could exploit this vulnerability to gain elevated privileges or cause the system to crash.

CVE-2024-22354 - IBM WebSphere Application Server 8.5, 9.0 and IBM WebSphere Application Server Liberty 17.0.0.3 through 24.0.0.5 are vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information, consume memory resources, or to conduct a server-side request forgery attack. IBM X-Force ID: 280401.

CVE-2023-6240 - Linux Kernel could allow a remote attacker to obtain sensitive information, caused by a Marvin vulnerability side-channel leakage in the RSA decryption operation. By exploiting the side-channel leakage, an attacker could exploit this vulnerability to decrypt ciphertexts or forge signatures, limiting the services that use that private key.

CVE-2023-52667 - Linux Kernel is vulnerable to a denial of service, caused by double-free in fs_any_create_groups of net/mlx5e. A local authenticated attacker could exploit this vulnerability to cause a denial of service.

CVE-2024-33601 - glibc is vulnerable to a denial of service, caused by a memory allocation failure when the Name Service Cache Daemon's (nscd) netgroup cache uses the xmalloc or xrealloc functions. A local attacker could exploit this vulnerability to terminate the daemon.

CVE-2024-22329 - IBM WebSphere Application Server 8.5, 9.0 and IBM WebSphere Application Server Liberty 17.0.0.3 through 24.0.0.3 are vulnerable to server-side request forgery (SSRF). By sending a specially crafted request, an attacker could exploit this vulnerability to conduct the SSRF attack. X-Force ID: 279951.

CVE-2023-52675 - Linux Kernel is vulnerable to a denial of service, caused by the lack of a null pointer check in update_events_in_group(). By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.

CVE-2024-26659 - Linux Kernel is vulnerable to a denial of service, caused by the improper handling of isoc Babble and Buffer Overrun events. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.

CVE-2024-26735 - Linux Kernel is vulnerable to a denial of service, caused by a use-after-free and NULL pointer dereference. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.

CVE-2024-25026 - IBM WebSphere Application Server 8.5, 9.0 and IBM WebSphere Application Server Liberty 17.0.0.3 through 24.0.0.4 are vulnerable to a denial of service, caused by sending a specially crafted request. A remote attacker could exploit this vulnerability to cause the server to consume memory resources. IBM X-Force ID: 281516.

CVE-2024-26602 - Linux Kernel is vulnerable to a denial of service, caused by an error related to sched/membarrier: reducing the ability to hammer on sys_membarrier. A local attacker could exploit this vulnerability to cause a denial of service.

CVE-2024-33599 - glibc is vulnerable to a stack-based buffer overflow, caused by improper bounds checking when the Name Service Cache Daemon's (nscd) fixed size cache is exhausted by client requests. By sending a subsequent client request, a remote attacker could exploit this vulnerability to overflow a buffer and execute arbitrary code on the system.

CVE-2023-52686 - Linux Kernel is vulnerable to a denial of service, caused by the lack of a null pointer check in opal_event_init(). By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.

CVE-2024-36004 - Linux Kernel is vulnerable to a denial of service, caused by the use WQ_MEM_RECLAIM flag for workqueue. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.

CVE-2023-52835 - Linux Kernel is vulnerable to a denial of service, caused by an out-of-bounds read. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.

CVE-2024-26585 - Linux Kernel is vulnerable to a denial of service, caused by a race condition when submitting thread in the tls subsystem. By sending a specially crafted request, a local attacker could exploit this vulnerability to cause a denial of service condition.

CVE-2024-33602 - glibc is vulnerable to a denial of service, caused by a memory corruption by the Name Service Cache Daemon's (nscd) netgroup cache when the NSS callback fails to store all strings in the provided buffer. A local attacker could exploit this vulnerability to corrupt memory and cause a denial of service.

CVE-2024-26993 - Linux Kernel is vulnerable to a denial of service, caused by a reference leak in sysfs_break_active_protection(). By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.

CVE-2024-33600 - glibc is vulnerable to a denial of service, caused by a NULL pointer dereference when the Name Service Cache Daemon's (nscd) cache fails to add a not-found netgroup response to the cache. A remote attacker could exploit this vulnerability to cause a denial of service.

CVE-2024-6387 - OpenSSH could allow a remote attacker to execute arbitrary code on the system, caused by a signal handler race condition. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary code with root privileges on glibc-based Linux systems.

CVE-2024-26583 - Linux Kernel is vulnerable to a denial of service, caused by a race condition in the tls subsystem. By sending a specially crafted request, a local attacker could exploit this vulnerability to cause a denial of service condition.

CVE-2024-26584 - Linux Kernel is vulnerable to a denial of service, caused by a flaw when setting the CRYPTO_TFM_REQ_MAY_BACKLOG flag on requests to the crypto API in the tls subsystem. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service condition.

CVE-2023-4244 - Linux Kernel could allow a local authenticated attacker to gain elevated privileges on the system, caused by a use-after-free flaw in the netfilter: nf_tables component. By sending a specially crafted request, an authenticated attacker could exploit this vulnerability to gain elevated privileges.

CVE-2024-0443 - Linux Kernel is vulnerable to a denial of service, caused by a flaw in the blkgs destruction path in block/blk-cgroup.c. A local authenticated attacker could exploit this vulnerability to cause system instability.

CVE-2024-26804 - Linux Kernel is vulnerable to a denial of service, caused by the failure to prevent perpetual headroom growth. A local authenticated attacker could exploit this vulnerability to cause a denial of service.

CVE-2024-26808 - Linux Kernel is vulnerable to a denial of service, caused by an error related to handling NETDEV_UNREGISTER for inet/ingress basechain. A local authenticated attacker could exploit this vulnerability to cause a denial of service.

CVE-2024-2961 - GNU C Library could allow a remote attacker to execute arbitrary code on the system, caused by an out-of-bounds write in the ISO-2022-CN-EXT plugin. By sending specially crafted input, an attacker could exploit this vulnerability to overwrite critical data structures and execute arbitrary code on the system or cause the application to crash.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale System	6.1.0.0-6.1.9.3
IBM Storage Scale System	6.2.0.0-6.2.0.1

Remediation/Fixes

For Storage Scale System, upgrade to 6.1.9.4 or 6.2.1.0 or later: [Link]

- **There are multiple vulnerabilities that can affect IBM Storage Scale System that are now included**

  Summary

  There are multiple vulnerabilities used by IBM Storage Scale System, which could provide weaker than expected security that are now fixed.

  Vulnerability Details

  CVE-2024-36005 - Linux Kernel is vulnerable to a denial of service, caused by an error related to netfilter: nf_tables: honor table dormant flag from netdev release event path. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.

  CVE-2021-46939 - Linux Kernel is vulnerable to a denial of service, caused by a flaw in the ring buffer recursion detection. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service condition.

  CVE-2024-36000 - Linux Kernel is vulnerable to a denial of service, caused by an error related to missing hugetlb_lock for resv uncharge. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.

  CVE-2023-52463 - Linux Kernel is vulnerable to a denial of service, caused by force RO when remounting if SetVariable is not supported. A local attacker could exploit this vulnerability to cause a denial of service.

  CVE-2024-26925 - Linux Kernel is vulnerable to a denial of service, caused by an error related to netfilter: nf_tables: release mutex after nft_gc_seq_end from abort path. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.

  CVE-2024-7348 - PostgreSQL could allow a remote authenticated attacker to gain elevated privileges on the system, caused by a tme-of-check time-of-use (TOCTOU) race condition in pg_dump. By sending a specially crafted request, an authenticated attacker could exploit this vulnerability to execute arbitrary SQL functions as the user running pg_dump.

  CVE-2024-36883 - Linux Kernel is vulnerable to a denial of service, caused by an out-of-bounds access in ops_init. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.

  CVE-2024-26665 - Linux Kernel is vulnerable to a denial of service caused by out-of-bounds access when building IPv6 PMTU. By sending a specially crafted request, a remote attacker could exploit this vulnerability to a denial of service condition.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale System	6.1.0.0 - 6.1.9.3
IBM Storage Scale System	6.2.0.0 - 6.2.1.0

[Link](#)

- **Storage Scale Software Version Recommendation Preventive Service Planning**

  IBM Storage Scale Software Version Recommendation

  Content

  > This generalised recommendation is made available to assist clients in implementing a code update strategy. It is a full field perspective, and as such, a customized recommendation that takes into account specifics such as business upgrade windows, length of time since last update, decommission plans. might require assistance from local support teams. In general, recommendations assume planning updates annually.

  Detailed information on the product fixes contained within IBM Storage Scale v5.x releases can be found here.

Version	Minimum Recommended Level	Latest Level
IBM Storage Scale		
	5.1.9.x stream2: 5.1.9.3 [Apr 2024]	5.1.9.x stream2: 5.1.9.6 [Sep 2024]
	5.2.x stream: 5.2.0.0 [Apr 2024]	5.2.x stream: 5.2.1.1 [Sep 2024]
IBM Storage Scale System (ESS)		
	5.1.x stream: ESS 6.1.9.2 [Mar 2024]	5.1.x stream: ESS 6.1.9.4 [Oct 2024]
IBM Storage Scale System 3000, 3200, 3500, 5000, and 6000		
	5.1.x stream: ESS 6.1.9.2 [Mar 2024]	5.1.x stream: ESS 6.1.9.4 [Oct 2024]
	5.2.x stream: ESS 6.2.0.1 [Jun 2024]	5.2.x stream: ESS 6.2.1.1 [Oct 2024]

[Link](#)

Keep safe and trust that the lead up to the end of year close-down is uneventful!
Red, Belisama