Belisama

January Newsletter

Subscribe/Unsubscribe

Greetings all,
I hope that '25 has got of to a good start and that you had a short break. Wishing you a safe and prosperous year of the snake.

A few updates to share

- Thanks to Chris (Mr Gibson) for collating a number of interesting updates from the IBM Power and AIX development teams (see below);
- Thanks to the IBM Champion team for recognising Belisama's efforts over the last 12 months promoting AIX and all things Power related and selecting me as an IBM Champion for another year.

Quick bites

Update multiple clients concurrently using `nimadm`
While this could be done using various hacks – from AIX 7.3.3.0 and above, multiple NIM clients can now be updated with `nimadm`. There is also a tutorial to take you through it
Link

Virtual Ethernet software multi queue
It has been found that the current version of the virtual ethernet driver is not scaling well in terms of bandwidth and latency as adapter speeds evolve to 100/200GbE. In AIX 7.3.3.0 and VIOS 4.1.1.0 the software multi queue feature is introduced and it is optimised to handle these new adapters and can offer up to 2x improvement in throughput and TPS.
Link

Server side caching (Power Flash Cache) in AIX 7.3.3.0
An AIX LPAR can now use SSDs/Flash Storage/NVMe drives/vPmem as read only cache to improve the performance of spinning disks. The command `cache_mgt` can be used to configure and active cache pools/partitions.
Link

Accelerate AIX IPsec with Power in core capability
Advanced Crypto Facility (ACF) is a cryptographic framework which provides crypto services for both AIX kernel and the user space applications and leverages the Power in-core hardware accelerator available starting from IBM Power 8 processor.
Link

User space Platform Key Store capability on AIX
Keeping user secrets secure is becoming increasing important – starting with FW950 and HMC 9.2.950 the Platform KeyStore (PKS) feature creates an ecrypted non-volatile store backed by NVRAM
Link

TCP Dynamic Socket Buffer Sizing (DSS)
To get optimum network performance it is often required to tune the `tcp_[send|recv]space`, which often required multiple iterations and is often host/connection specific. The dynamic socket buffer sizing feature is introduced in AIX 7.3.3.0 and dynamically adjusts the socket buffer sizes for each connection based on the bandwidth / latency for each host connection.
Link
AIX 16MB Text Page Promotion
Large page optimisation is a feature of ASO (AIX dynamic system optimiser) that promotes the page size from 4/64KB to 16MB when:

- The size of process text must be greater than 16 MB.
- The base page size of the process text must be 64 KB.
- The process must be running in 64-bit environment
- The process must have a runtime exceeding 10 minutes.
- The cumulative CPU utilisation of all processes sharing the same text must be high.

This optimisation potentially improves the performance of workloads that use those regions because it reduces the number of TLB misses. Prior to AIX 7.3.3.0 only System V shared memory was eligible, now it applies to test pages as well.
Link
Non-root user updating firmware on non-HMC managed systems
Non-HMC managed systems can have their firmware updated by root using the `diag` command or the `update_flash` utility. This raises potential security concerns, but starting with AIX 7.3.3.0, a designated non-root user can update and view system firmware.
Link
Performing a live kernel updates with active IPsec tunnels
Protecting data in flight is essential, and IPsec is one way in AIX to achieve this. Thus it must be kept running at all times – including during service windows / system upgrades. This blog will provide further information on migrating IPsec with live kernel update.
Link
AIX time zone update tool
This perl scripted tool available in AIX 7.3.3.0 streamlines the process of updating AIX time zone rules whenever there is a modification of DST changes from IANA (the standards body that maintains the Olson time zone rules globally).
Link
RoCEv2 support on AIX
RoCEv1 provides RDMA over ethernet layer 2 network and the header cannot be understood by layer 3 switches. RoCEv2 packets carry an IP header which allows traversal of IP L3 Routers and a UDP header that serves as a stateless encapsulation layer for the RDMA Transport Protocol Packets over IP.
Link
AIX 7.3 Installation Tips
This document contains tips for successful installation of AIX 7.3 and is updated as new tips become available (Last Update: 13 January 2025).
Link

AIX 7.3.3.0 bulk DMA unmap feature
AIX read/write operations to block I/O devices use DMA (Direct Memory Access). Prior to AIX 7.3.3.0 this was mapped/unmapped on the fly using expensive hypervisor calls, thus creating a bottleneck and limiting IOPS.
Link
AIX audit API enhancements
The audit subsystem captures important security related information, which can then be analysed to detect potential and actual violations of the system's security policy. In AIX 7.3.3.0, two new flags have been added to improve the functionality and ease of use of the audit subsystem.
Link
AIX audit support for live kernel update
Currently AIX audit only supports live kernel update if in BIN mode, not STREAM mode. In AIX 7.3.3.0, support is introduced for audit in both BIN and STREAM mode and the `watch` command was introduced to observe a programme during live kernel update.
Link
Need to update your AIX skills?
AIX Basics – for this course IBM offers a variety of delivery mechanisms – instructor lead or self paced / online and the option of a Badge. Explore the learning paths for AIX Operator, AIX Administrator and AIX Developer.
Link
VIO Server and Python, a short history
Andrey looks at managing your VIO Server using Ansible and addresses the issue that prior to VIO Server 4, python was not available. VIO Server 4.1.1 has two versions – 3.9 and 3.11 – but what if you want another version?
The answer is you install Python* – and Andrey looks as using Ansible to perform this task.
* Python is not in the list of software you are allowed to install – but many users have (including me) and it is installed by default in version 4+.
Link
Gathering data from the Surrogate LPAR after a failed Live Update.
Sometimes when Live Update fails due to a problem on the Surrogate LPAR, the logs from the Surrogate LPAR are not copied over on the remaining Original LPAR and manual extraction is required.
Link
Power9 Performance Best Practices
IBM Support has updated their "Power9 Performance Best Practices" – for all versions of AIX. This document is intended as a short summary for customers on key items that should be looked at when using Power9 hardware and includes links to a more in depth and complete set of recommendations.
Link

Coming soon

- **ASEANZK AIX/IBM i/Linux on Power Meetup Group**
  What this space – we are looking around for topics and speakers (suggestions welcome!) and hope to launch the ‘25 programme soon.
  Link

Redbooks and Redpapers

- **Introduction to IBM Power Virtual Server Private Cloud**, Draft Redpaper, 29 January 2025,
  Link
- **IBM Power Systems Virtual Server Guide for IBM i**, Draft Redbook, 14 January 2025,
  Link

IBM alerts and notices

Java alerts and updates:

- **Java SDK security vulnerabilities**
  A list of recent Security Vulnerabilities addressed in the Developer Kits currently available from our downloads page. IBM customers requiring these fixes in a binary IBM Java SDK/JRE for use with an IBM product should contact IBM Support and engage the appropriate product service team.
  Link
- **Add amazon root certificates to IBM Java's cacerts: IJ53251**
  Four Amazon root certs have been added.
  Downloads and supplementary documentation can be found at the following locations:
  For non z/OS operating systems:
  IBM Semeru Runtimes, Version 11 and later:
  https://www.ibm.com/semeru-runtimes/downloads/
  IBM SDK, Java Technology Edition, Version 8:
  https://www.ibm.com/support/pages/java-sdk-downloads/
  Link
- **TZ updates in IBM Semeru runtimes and IBM SDK Java TE**
  See link for details
  Link
- **IBM TZ update utility for Java**
  The IBM Time Zone Update Utility for Java (JTZU) applies Daylight Saving Time (DST) changes directly to your Java SDKs and JREs.
  Link

AIX alerts and updates:

- **AIX is vulnerable to denial of service (CVE-2024-47102, CVE-2024-52906)**

Vulnerabilities in the AIX TCP/IP and perfstat kernel extensions may lead to a denial of service (CVE-2024-47102, CVE-2024-52906).

Vulnerability Details

CVE-2024-47102 - IBM AIX could allow a non-privileged local user to exploit a vulnerability in the AIX perfstat kernel extension to cause a denial of service.

CVE-2024-52906 - IBM AIX could allow a non-privileged local user to exploit a vulnerability in the TCP/IP kernel extension to cause a denial of service.

Affected Products and Versions

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

Link

- **AIX Service Pack 7200-05-09-2446**

Service Packs contain important fixes delivered between Technology Levels. Service Pack 7200-05-09-2446 is based on Technology Level 7200-05.

Link

- **AIX 7.2 TL5 PEs Fixed In 7200-05-09-2446**

This is a list of identified PTFs in Error (PEs) for AIX 7.2 Technology Level 7200-05 that are fixed in Service Pack 7200-05-09-2446**.**

Link

- **AIX Technology Level 7300-03**

Technology Level (TL) 7300-03 for AIX 7.3 contains preventive maintenance, new software features, and support for new hardware.

Link

- **AIX Technology Level 7300-03**

Download fixed and drivers.

Link

- **AIX is vulnerable to a denial of service due to libxml2 (CVE-2024-25062)**

Vulnerability in libxml2 could allow a remote attacker to cause a denial of service (CVE-2024-25062). AIX uses libxml2 as part of its XML parsing functions.

Vulnerability Details

CVE-2024-25062 - An issue was discovered in libxml2 before 2.11.7 and 2.12.x before 2.12.5. When using the XML Reader interface with DTD validation and XInclude expansion enabled, processing crafted XML documents can lead to an xmlValidatePopElement use-after-free.

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
bos.rte.control	7.2.5.0	7.2.5.102
bos.rte.control	7.2.5.200	7.2.5.202
bos.rte.control	7.3.0.0	7.3.0.3
bos.rte.control	7.3.1.0	7.3.1.2
bos.rte.control	7.3.2.0	7.3.2.0

IBM has assigned the following APARs to this problem:

AIX Level	APAR	SP
7.2.5	IJ50602	SP08
7.3.0	IJ50827	N/A
7.3.1	IJ50635	SP04
7.3.2	IJ50601	SP02
VIOS Level	APAR	FP
3.1.3	IJ50828	N/A
3.1.4	IJ50602	3.1.4.40
4.1.0	IJ50601	4.1.0.20

Link

PowerVM alerts and updates:

- **VIOS 3.1.4.50**
  Download fixes and drivers
  Link
- **VIOS 4.1.1.0**
  Download fixes and drivers
  Link

High Impact / Highly Pervasive (HIPER):

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

  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

  Affected Domain

  LPARs using NPIV with certain Fibre Channel adapters

  Note: On 12/11/24 the adapter microcode update became available, and the Recommended Action below was updated accordingly.

  The following command on the VIOS will report the Feature Code for these above adapters. Note: the output may be blank for other FC adapters.

  ```
  $ lsdev -dev fcs# -vpd | grep "Feature Code"
  ```

  This issue with the adapter microcode 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)

Presence of a fix for IJ47358/IJ49879 on the VIOS can be identified by running either:

```
$ instfix -ik IJ47358  #for 3.1.4
$ instfix -ik IJ49879  #for 4.1.0
```

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.

Recommended Action

To prevent the issues described above, apply the corresponding adapter microcode updates below to any affected adapter:

Adapter Feature Code	Microcode level
EN1E/EN1F	7710712014109e06.070205
EN1G/EN1H	7710612214105006.070205
EN1J/EN1K	7710812214105106.070120
EN2L/EN2M	771089201410c606.070B08
EN2N/EN2P	771089221410c506.070B08

Note: after applying the adapter microcode, remove any temporary VIOS ifix labeled 'cv31441s1a' or 'cv41021s1a' if one was previously applied.

Link

Hardware:

- **Power9 life cycle information**

Life cycle updates for the following servers:

- IBM Power System S922 Server (9009-22A)
- IBM Power System H924 Server (9223-42H)
- IBM Power System H922 Server (9223-22H)
- IBM Power System S924 Server (9009-42A)
- IBM Power System L922 Server (9008-22L)

Further information

Life cycle	Date	announcement letter
GA:	20-Mar-2018	118-022
EOM:	29-Jan-2021	920-152
EOS:	31-Jan-2026	AD25-0134

Link

- **New Power10 firmware for ML1050, MM1050**

The latest service pack 1050.23 is now available for system firmware levels, ML1050 and MM1050.

Security problem was fixed for CVE-2024-41007

Security problems were fixed for CVE-2023-52340 and CVE-2023-52881

Risk Classification	Product / Component	Platform / Version
HIPER	E1050 (9043-MRX)	All platforms / versions
HIPER	L1022 (9786-22H)	All platforms / versions
HIPER	L1024 (9786-42H)	All platforms / versions
HIPER	S1014 (9105-41B)	All platforms / versions
HIPER	S1022 (9105-22A)	All platforms / versions

HIPER	S1022s (9105-22B)	All platforms / versions

Link

- **New Power10 firmware for VL950, VM950, and VH950**
  The latest service pack 950.C2 is now available for system firmware levels VL950, VM950, and VH950.

Risk Classification	Product / Component	Platform / Version
HIPER	S914 (9009-41G)	All platforms / versions
HIPER	E950 Server (9040-MR9)	All platforms / versions
HIPER	E980 Server (9080-M9S)	All platforms / versions
HIPER	H922 Server (9223-22H)	All platforms / versions
HIPER	H922 Server (9223-22S)	All platforms / versions
HIPER	H924 Server (9223-42H)	All platforms / versions
HIPER	H924 Server (9223-42S)	All platforms / versions
HIPER	L922 Server (9008-22L)	All platforms / versions
HIPER	S914 Server (9009-41A)	All platforms / versions
HIPER	S922 Server (9009-22A)	All platforms / versions
HIPER	S922 Server (9009-22G)	All platforms / versions
HIPER	S924 Server (9009-42A)	All platforms / versions
HIPER	S924 Server (9009-42G)	All platforms / versions

Link

ESS / GPFS (Scale):

- **mmfsck hits SIG 11 issue**
  NB: Fix is coming, see link
  Link
- **Storage Scale System has identified an issue in drive firmware that may cause a drive to be marked as failed**
  Recently, a defect was identified in some of the IBM Storage Scale System drive firmware. After a drive firmware update, a head alignment process is initiated, which can take up to 4 hours to complete. During this alignment process, the drive heads might not be perfectly aligned, potentially leading to retries, performance issues, and intervention by GNR disk hospital. In severe cases, the drive may be flagged as failed due to excessively high bit error rates, checksum errors, or insufficient overall performance. It's important to note that this process does not inherently lead to data corruption or loss.
  Users Affected
  Users upgrading to the following drive firmware levels are affected:
  SCP2, TCP2, SCP4, TCP4, SCP5, TCP5, SCP8, TCP8
  SCL2, NCL2, SCL3, NCL3, SCL4, NCL4, SCL6, NCL6
  This can be hit on Storage Scale System 5000 running all currently supported code levels (Storage Scale System 6.1.0.0 through 6.1.9.4 and Storage Scale System 6.2.0.0 through 6.2.1.1).
  Problem Determination

Run the following command to see if the system drives have the affected firmware:

```
mmlsfirmware --type drive
```

Link

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

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

Vulnerability Details

CVE-2023-52451 - Linux Kernel is vulnerable to a denial of service, caused by an error related to access beyond end of drmem array. A local attacker could exploit this vulnerability to cause a denial of service.

CVE-2024-41076 - Linux Kernel is vulnerable to a denial of service, caused by a flaw in NFSv4. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.

CVE-2024-35890 - Linux Kernel is vulnerable to a denial of service, caused by a ownership transfer issue if packets are GROed with fraglist. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service condition.

CVE-2024-42131 - In the Linux kernel, the following vulnerability has been resolved: mm: avoid overflows in dirty throttling logic The dirty throttling logic is interspersed with assumptions that dirty limits in PAGE_SIZE units fit into 32-bit (so that various multiplications fit into 64-bits). If limits end up being larger, we will hit overflows, possible divisions by 0 etc. Fix these problems by never allowing so large dirty limits as they have dubious practical value anyway. For dirty_bytes / dirty_background_bytes interfaces we can just refuse to set so large limits. For dirty_ratio / dirty_background_ratio it isn't so simple as the dirty limit is computed from the amount of available memory which can change due to memory hotplug etc. So when converting dirty limits from ratios to numbers of pages, we just don't allow the result to exceed UINT_MAX. This is root-only triggerable problem which occurs when the operator sets dirty limits to >16 TB.

CVE-2024-26783 - The Linux Kernel is vulnerable to a denial of service, which is caused by calling wakeup_kswapd() with a wrong zone index. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.

CVE-2024-40995- Linux Kernel is vulnerable to a denial of service, caused by an infinite loop in Tcf_idr_check_alloc(). By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale System	6.1.9.0 - 6.1.9.3

IBM Storage Scale System 6.2.0.0 - 6.2.0.1

Link

- **Multiple Linux Kernel vulnerabilities may affect IBM Storage Scale System**

There are multiple vulnerabilities in the Linux kernel, used by IBM Storage Scale System, which could allow a denial of service. Fixes for these vulnerabilities are available.

Vulnerability Details

CVE-2024-40998 - Linux Kernel is vulnerable to a denial of service, caused by uninitialized Ratelimit_state->Lock Access in __ext4_fill_super(). By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.

CVE-2024-0641 - Linux Kernel is vulnerable to a denial of service, caused by a flaw in tipc_crypto_key_revoke in net/tipc/crypto.c in the TIPC subsystem. A local authenticated attacker could exploit this vulnerability to trigger a deadlock and potentially crash the system.

CVE-2024-0340 - Linux Kernel could allow a local authenticated attacker to obtain sensitive information, caused by a flaw in the vhost_new_msg function in drivers/vhost/vhost.c. By reading the /dev/vhost-net device file, an attacker could exploit this vulnerability to obtain kernel memory information, and use this information to launch further attacks against the affected system.

CVE-2024-40958 - Linux Kernel is vulnerable to a denial of service, caused by a use-after-free in net_namespace.c. A local authenticated attacker could exploit this vulnerability to cause a denial of service.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale System	6.1.0.0 - 6.1.9.4
IBM Storage Scale System	6.2.0.0 - 6.2.1.1

Link

- **IBM Storage Scale System may be affected by vulnerabilities in OpenSSL**

Security vulnerabilities have been discovered in OpenSSL that are now fixed.

Vulnerability Details

CVE-2023-3446 - OpenSSL is vulnerable to a denial of service, caused by a flaw when using the DH_check(), DH_check_ex() or EVP_PKEY_param_check() functions to check a DH key or DH parameters. By sending a specially crafted request using long DH keys or parameters, a remote attacker could exploit this vulnerability to cause long delays, and results in a denial of service condition.

CVE-2023-3817

DESCRIPTION: OpenSSL is vulnerable to a denial of service, caused by a flaw when using the DH_check(), DH_check_ex() or EVP_PKEY_param_check() functions to check a DH key or DH parameters. By sending a specially crafted request, a remote attacker could exploit this vulnerability to cause long delays, and results in a denial of service condition.

CVE-2023-5678 - Openssl is vulnerable to a denial of service, caused by a flaw when using DH_generate_key() function to generate an X9.42 DH key. By sending a

specially crafted request, a remote attacker could exploit this vulnerability to cause a denial of service condition.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale System	6.1.9.0 - 6.1.9.4
IBM Storage Scale System	6.2.0.0 - 6.2.1.1

Link

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

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

Vulnerability Details

CVE-2024-36889 - Linux Kernel is vulnerable to a denial of service, caused by the failure to ensure snd_nxt is properly initialized on connect. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.

CVE-2024-26629 - Linux Kernel is vulnerable to a denial of service, caused by a flaw in the nfsd4_release_lockowner() function. A local authenticated attacker could exploit this vulnerability to cause a denial of service.

CVE-2024-0841 - Linux Kernel could allow a local authenticated attacker to gain elevated privileges on the system, caused by a NULL pointer dereference flaw in the hugetlbfs_fill_super function in the hugetlbfs (HugeTLB pages) functionality. By sending a specially crafted request, an authenticated attacker could exploit this vulnerability to gain elevated privileges or cause the system to crash.

CVE-2023-52455 - Linux Kernel is vulnerable to a denial of service, caused by the failure to reserve 0-length IOVA region. A local attacker could exploit this vulnerability to cause a denial of service.

CVE-2021-47289 - Linux Kernel is vulnerable to a denial of service, caused by a null pointer dereference in ACPI. A local authenticated attacker could exploit this vulnerability to cause a denial of service.

CVE-2023-52489 - Linux Kernel is vulnerable to a denial of service, caused by a race condition in accessing memory_section->usage. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service condition.

CVE-2024-41064 - Linux Kernel is vulnerable to a denial of service, caused by a flaw in Powerpc/Eeh. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.

CVE-2023-0597 - Linux Kernel could allow a local attacker to obtain sensitive information, caused by a memory leak in the cpu_entry_area mapping of X86 CPU data to memory. An attacker could exploit this vulnerability to gain access to some important data with expected location in memory.

CVE-2024-40972 - Linux Kernel is vulnerable to a denial of service, caused by a flaw in ext4. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.
CVE-2023-2269 - Linux Kernel is vulnerable to a denial of service, caused by a deadlock in the table_clear function in the Device Mapper-Multipathing sub-component in drivers/md/dm-ioctl.c. By sending a specially crafted request, a local attacker could exploit this vulnerability to cause a denial of service condition.
CVE-2023-42754 - Linux Kernel is vulnerable to a denial of service, caused by a NULL pointer dereference flaw in the ipv4_send_dest_unreach function in net/ipv4/route.c. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service condition.
CVE-2023-3161 - Linux Kernel is vulnerable to a denial of service, caused by a shift-out-of-bounds flaw in the fbcon_set_font() function. By sending a specially crafted request, a remote attacker could exploit this vulnerability to cause a denial of service condition.
CVE-2024-26633 - Linux Kernel is vulnerable to a denial of service, caused by an error related to NEXTHDR_FRAGMENT handling in ip6_tnl_parse_tlv_enc_lim(). A local authenticated attacker could exploit this vulnerability to cause a denial of service.
CVE-2024-26671 - Linux Kernel is vulnerable to a denial of service, caused by a race condition in the blk_mq_mark_tag_wait() function. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service condition.
CVE-2023-1077 - Linux Kernel is vulnerable to a denial of service, caused by a type confusion flaw in the pick_next_rt_entity() function in the RT scheduling stack. By sending a specially-crafted request, a local attacker could exploit this vulnerability to cause a denial of service condition.
CVE-2024-42152 - Linux Kernel is vulnerable to a denial of service, caused by memory leak in nvmet. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service condition.
CVE-2024-41055 - Linux Kernel is vulnerable to a denial of service, caused by Null pointer dereference in mmzone.h. A local authenticated attacker could exploit this vulnerability to cause a denial of service.
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.
CVE-2023-52581 - Linux Kernel could allow a local authenticated attacker to execute arbitrary code on the system, caused by a memory leak when more than 255 elements expired. By sending a specially crafted request, an attacker

could exploit this vulnerability to execute arbitrary code or cause the system to crash.
CVE-2023-3640 - Linux Kernel could allow a local authenticated attacker to gain elevated privileges on the system, caused by unauthorized memory access flaw in cpu_entry_area mapping of X86 CPU data to memory. By sending a specially crafted request, an authenticated attacker could exploit this vulnerability to gain elevated privileges.
CVE-2024-38601 - Linux Kernel is vulnerable to a denial of service, caused by a flaw in Ring-Buffer. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.
CVE-2024-10979 - PostgreSQL could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an incorrect control of environment variables flaw. By changing sensitive process environment variables, an attacker could exploit this vulnerability to execute arbitrary code on the system.
CVE-2024-21147 - An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause high confidentiality, high integrity impacts.
CVE-2024-21145 - An unspecified vulnerability in Java SE related to the 2D component could allow a remote attacker to cause low confidentiality, low integrity impacts.
CVE-2024-21140 - An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause low confidentiality, low integrity impacts.
CVE-2024-21138 - An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause a low availability impact.
CVE-2024-21131 - An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause low integrity impact.
CVE-2024-26640 - Linux Kernel is vulnerable to a denial of service, caused by the lack of sanity checks to rx zerocopy. A local authenticated attacker could exploit this vulnerability to cause a denial of service.
CVE-2023-52474 - Linux Kernel is vulnerable to a denial of service, caused by an error related to non-PAGE_SIZE-end multi-iovec user SDMA requests. A local attacker could exploit this vulnerability to cause a denial of service.
CVE-2023-52610 - Linux Kernel is vulnerable to a denial of service, caused by an skb leak and crash on ooo frags. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.
CVE-2023-52472 - Linux Kernel is vulnerable to a denial of service, caused by a NULL pointer dereference in crypto. A local attacker could exploit this vulnerability to cause a denial of service.
CVE-2023-6915 - Linux Kernel is vulnerable to a denial of service, caused by a NULL pointer dereference flaw in the ida_free function in lib/idr.c. By

sending a specially crafted request, a remote authenticated attacker could exploit this vulnerability to cause a denial of service condition.
CVE-2023-52476 - Linux Kernel is vulnerable to a denial of service, caused by a panic can occur when a vsyscall is made while LBR sampling is active. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service condition.
CVE-2024-24855 - Linux Kernel is vulnerable to a denial of service, caused by a race condition in the lpfc_unregister_fcf_rescan() function in the scsi device driver. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a kernel panic or a denial of service condition.
CVE-2024-26826 - Linux Kernel is vulnerable to a denial of service, caused by an error related to data re-injection from stale subflow. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.
CVE-2023-1206 - Linux Kernel is vulnerable to a denial of service, caused by a flaw in the IPv6 connection lookup table. By sending a specially crafted request, a remote attacker could exploit this vulnerability to cause the CPU usage to increase, and results in a denial of service condition.
CVE-2023-52580 - Linux Kernel is vulnerable to a denial of service, caused by an incorrect calculation of buffer size in ETH_P_1588 flow dissector. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service condition.
CVE-2024-40978 - Linux Kernel is vulnerable to a denial of service, caused by a flaw in Scsi: Qedi. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.
CVE-2024-40954 - In the Linux kernel, the following vulnerability has been resolved: net: do not leave a dangling sk pointer, when socket creation fails It is possible to trigger a use-after-free by: * attaching an fentry probe to __sock_release() and the probe calling the bpf_get_socket_cookie() helper * running traceroute -I 1.1.1.1 on a freshly booted VM A KASAN enabled kernel will log a BUG – see link for details.
CVE-2023-52620- Linux Kernel is vulnerable to a denial of service, caused by a resource injection flaw in timeout parameter in nf_tables. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service condition.
CVE-2024-40959 - Linux Kernel is vulnerable to a denial of service, caused by a Null pointer dereference xfrm6_get_saddr() ip6_dst_idev(). A local authenticated attacker could exploit this vulnerability to cause a denial of service.
CVE-2023-3268 - Linux Kernel is vulnerable to a denial of service, caused by an out-of-bounds memory access flaw in the relay_file_read_start_pos function in kernel/relay.c in the relayfs. By sending a specially crafted

request, a local authenticated attacker could exploit this vulnerability to cause the system to crash or obtain sensitive information.
CVE-2023-39194 - Linux Kernel could allow a local authenticated attacker to obtain sensitive information, caused by an out-of-bounds read flaw in the processing of state filters in XFRM. By sending a specially crafted request, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.
CVE-2023-45863 - Linux Kernel could allow a local authenticated attacker to execute arbitrary code on the system, caused by a race condition that results in a fill_kobj_path out-of-bounds write in lib/kobject.c. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition.
CVE-2024-40960 - Linux Kernel is vulnerable to a denial of service, caused by a NULL Dereference in Rt6_probe(). By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.
CVE-2023-6622 - Linux Kernel is vulnerable to a denial of service, caused by a NULL pointer dereference flaw in the nft_dynset_init() function in net/netfilter/nft_dynset.c. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service condition.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale System	6.1.9.0 - 6.1.9.4
IBM Storage Scale System	6.2.0.0 - 6.2.1.1

Link

- **Software Version Recommendation Preventive Service Planning**

IBM Storage Scale Software Version Recommendation
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 customised 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.

IBM Storage Scale	Min Recommended Level	Latest Level
IBM Storage Scale	5.1.9.x stream2: 5.1.9.3 [Apr 2024] 5.2.x stream: 5.2.0.0 [Apr 2024]	5.1.9.x stream2: 5.1.9.7 [Nov 2024] 5.2.x stream: 5.2.2.0 [Dec 2024]
IBM Storage Scale System (ESS)	5.1.x stream: ESS 6.1.9.2 [Mar 2024]	5.1.x stream: ESS 6.1.9.5 [Dec 2024]
IBM Storage Scale System 3000, 3200, 3500, 5000 and 6000	5.1.x stream: ESS 6.1.9.2 [Mar 2024] 5.2.x stream: ESS 6.2.0.1 [Jun 2024]	5.1.x stream: ESS 6.1.9.5 [Dec 2024] 5.2.x stream: ESS 6.2.1.1 [Oct 2024]

IBM Storage Scale Container Native Storage Access (CNSA) IBM Storage Scale Container Storage Interface (CSI) (stand-alone)	5.1.9 stream: 5.1.9.7 [Nov 2024] 2.10.x stream: 2.10.5 [Nov 2024]	5.2.x stream: 5.2.2.0 [Dec 2024] 2.13.x stream: 2.13.0 [Dec 2024]

Link

Keep safe and hope that the above information was useful for your planning.
Red, Belisama