Belisama

March Newsletter

Subscribe/Unsubscribe

Greetings all,
Wishing you a happy Eid and trust that you will have a bit of time off during the Easter break.

A few updates to share

- Hoping to avoid my usual last minute rush and starting to work on my presentations for TechXchange – see below for details for this year's event.
- Are you tired of just hearing about OpenShift, and want to dip your toe in the "containers on Power" pond, without the overhead? Andrey looks at the way to start small with containers as a new way to run your workloads on Power.
  Link

Quick bites

Optimising JFS on AIX
Anand Kumar put together a good article delving into the tricks of of optimising JFS to tune its performance and efficiency.
Link

Updating VIOs to 4.1
This can be a real pain, but Andrey looks at how to simplify the upgrade.
Link

Intel x86, IBM Power, and Containers: A Unified IT Infrastructure.
A fresh take on the hybrid infrastructure use in your data centre and worth a read.
I am not sure that I would use "trucks" as the analogy for Power Servers, (perhaps hyperspace cruisers??), anyway still a good overview.
Link

IBM TechXchange Conference 2025
Early Bird pricing available for a limited time - The IBM TechXchange Conference 2025 is scheduled for October 6-9, 2025, at the Orange County Convention Centre in Orlando, Florida.
Link

Testcase Data Exchange – New ECuRep server replacing Testcase server in the US
The testcase server will be replaced by a new ECuRep server in the US on 20th March 2025
Link

In case you missed ….

- **PowerVM AIX: The 6 Layers of the PowerVM CPU nomenclature at SMT8**
  with Earl Jew and Chip Layton
  This session started with a conceptual explanation of each layer of the PowerVM CPU nomenclature then covers the concept of CPUtime recycling at SMT8. This session is based what AIX shows us about each layer supporting AIX-on-PowerVM. Understanding this structure is key to understanding the practical steps that will be covered in following sessions
  Link

Coming soon

- **IBM TechXchange Conference 2025**
  See above

Redbooks and Redpapers

- **IBM Power Virtual Server Guide for IBM AIX and Linux**
  Draft Redbooks, published: 11 March 2025
  Link
- **IBM Power 10 Scale Out Servers Technical Overview S1012, S1014, S1022s, S1022 and S1024**, Redpaper, published: 01 March 2025
  Link

IBM alerts and notices

PowerVM HIPER:

- **IJ53478: VIO client I/O may hang or fail**
  On VIOS 4.1.1.0, VIO client I/O may hang, escalating to path loss and potential I/O failures. We have seen this mainly with Linux clients running high I/O workloads, including SAP HANA.
  Recommended Action – apply the ifix
  Link

AIX alerts:

- **AIX is vulnerable to arbitrary command execution**

  Vulnerabilities in AIX could allow a remote attacker to execute arbitrary commands (CVE-2024-56346, CVE-2024-56347).

  Vulnerability Details

  CVE-2024-56346 - IBM AIX nimesis NIM master service could allow a remote attacker to execute arbitrary commands due to improper process controls.

  CVE-2024-56347 - IBM AIX nimsh service SSL/TLS protection mechanisms could allow a remote attacker to execute arbitrary commands due to improper process controls.

  Affected Products and Versions

Affected Product(s)	Version(s)
AIX	7.2
AIX	7.3

  The vulnerabilities in the following filesets are being addressed:

Fileset	Lower Level	Upper Level
bos.sysmgt.nim.client	7.2.5.0	7.2.5.203
bos.sysmgt.nim.master	7.2.5.0	7.2.5.204
bos.sysmgt.sysbr	7.2.5.0	7.2.5.203
bos.sysmgt.nim.client	7.3.1.0	7.3.1.3
bos.sysmgt.nim.master	7.3.1.0	7.3.1.3
bos.sysmgt.sysbr	7.3.1.0	7.3.1.3
bos.sysmgt.nim.client	7.3.2.0	7.3.2.2
bos.sysmgt.nim.master	7.3.2.0	7.3.2.2
bos.sysmgt.sysbr	7.3.2.0	7.3.2.2
bos.sysmgt.nim.client	7.3.3.0	7.3.3.0
bos.sysmgt.nim.master	7.3.3.0	7.3.3.0
bos.sysmgt.sysbr	7.3.3.0	7.3.3.0

  Link

- **AIX is vulnerable to a denial of service**

  Vulnerabilities in AIX's OpenSSH could allow a remote attacker to cause a denial of service (CVE-2025-26466) or a machine-in-the-middle attack (CVE-2025-26465). OpenSSH is used by AIX for remote login.

  Vulnerability Details

  CVE-2025-26466 - A flaw was found in the OpenSSH package. For each ping packet the SSH server receives, a pong packet is allocated in a memory buffer and stored in a queue of packages. It is only freed when the server/client key exchange has finished. A malicious client may keep sending such packages, leading to an uncontrolled increase in memory consumption on the server side. Consequently, the server may become unavailable, resulting in a denial of service attack.

  CVE-2025-26465 - A vulnerability was found in OpenSSH when the VerifyHostKeyDNS option is enabled. A machine-in-the-middle attack can be

performed by a malicious machine impersonating a legit server. This issue occurs due to how OpenSSH mishandles error codes in specific conditions when verifying the host key. For an attack to be considered successful, the attacker needs to manage to exhaust the client's memory resource first, turning the attack complexity high.

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
openssh.base.client	9.2.112.0	9.7.3013.1000
openssh.base.server	9.2.112.0	9.7.3013.1000
openssh.base.client	9.9.3015.1000	9.9.3015.1000
openssh.base.server	9.9.3015.1000	9.9.3015.1000

Link

- **AIX is affected by a denial of service (CVE-2024-50602) due to Python**

Summary

Vulnerability in Python could allow a remote attacker to cause a denial of service (CVE-2024-50602). Python is used by AIX as part of Ansible node management automation.

Vulnerability Details

CVE-2024-50602 - An issue was discovered in libexpat before 2.6.4. There is a crash within the XML_ResumeParser function because XML_StopParser can stop/suspend an unstarted parser.

Affected Products and Versions

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

The following fileset levels are vulnerable:

Fileset	Lower Level	Upper Level
python3.9.base	3.9.0.0	3.9.20.0

Link

AIX Update:

- **IJ54046: HTTPS CHANNEL BINDING SUPPORT**

Support has been added for TLS channel binding tokens for Negotiate/Kerberos authentication over HTTPS through javax.net.HttpsURLConnection.

Channel binding tokens are increasingly required as an enhanced form of security. They work by communicating from a client to a server the client's understanding of the binding between connection security, as represented by a TLS server cert, and

higher level authentication credentials, such as a username and password. The server can then detect if the client has been fooled
by a MITM (Man In The Middle) and shutdown the session or connection. The feature is controlled through a new system property `jdk.https.negotiate.cbt` which is described fully in <OSB>Networking Properties
Link

AIX notices:

- **Configure Rsyslog Server to Implement Client-Based Log Separation**
  Summary
  This document explains how to configure centralised log server to store log messages which are forwarded from remote syslog/rsyslog clients, in client specific log files, in attempt to override the default behaviour of accumulating log messages from different sources in one single log file.
  Objective
  Set up AIX rsyslog server to store the remote logs in local log files, one file per client and will involve downloadoing the AIX rsyslog code and making some changes to the rsyslog.conf file. This note also explains how rsyslog is designed and the modules used.
  Link

Storage HIPER:

- **An issue with IBM Flash Core Modules in IBM Storage Scale System 6000 could lead to detected data loss**
  IBM has identified an issue in IBM Storage Scale System 6.2.0.0 through 6.2.2.0 code, where detected data loss can occur in an IBM Storage Scale System 6000 that uses IBM Flash Core Modules (FCM).
  Description
  During node initialisation, Linux may reset the NVMe controllers and perform a device discovery. As part of the discovery, Linux sends a wide range of NVMe identify administrator commands to find attached devices. These discovery activities are typically performed during Linux start or recovery of an unresponsive device.
  FCMs do not support all NVMe identify commands. When an FCM device rejects an unsupported identify commands, it can expose an issue that may result is a misread or miswrite as follows:
  While the unsupported command that is being rejected is received from one port, read or write commands received through the other port of the same drive may return incorrect data from the drive (transient misread) or write incorrect data to the media (miswrite).
  Read or write operation from one canister while the peer canister is initialising (booting) or a device being recovered may be subjected to this exposure.

GNR implements a strong and powerful data validation strategy and will automatically recover most of the misread events:
Both data and its associated metadata have a checksum stored with the data in the FCM media during a write operation.
The checksum is checked and validated during read operation or background scrub operations.
When a misread happens, GNR can detect it during the checksum validation, and corrects the incorrect data by recreating data and writing it. GNR logs all incorrect checksum events.
In very rare occasions, GNR might not be able to recreate the data (and therefore correct the media) due to checksum errors observed from multiple drives exceeding the redundancy (that is, three errors in the same 8+2P RAID stripe) and will return an error to the host request. The requested data might be permanently lost.

Users Affected:

This issue may affect clients that use all of the following:

IBM Storage Scale System 6000 with FCM
IBM Storage Scale System 6.2.0.0 through 6.2.2.0
FCM firmware at 4_1_10 or lower version

Link

- **Potential silent corruption of data that impacts Erasure Code Edition and IBM Storage Scale Systems**

IBM has identified an issue in IBM Storage Scale 5.1.7.0 - 5.1.9.8 (IBM Storage Scale System 6.1.8.0 - 6.1.9.5) and IBM Storage Scale 5.2.0.0 - 5.2.2.0 (IBM Storage Scale System 6.2.0.0 - 6.2.2.0) that impacts IBM Storage Scale Erasure Code Edition (IBM Storage Scale ECE) and IBM Storage Scale System. The issue is a race condition that involves multiple threads performing a full-track read operation to the same track while disk errors exist. When the configuration parameter nsdRAIDClientOnlyChecksum is enabled, this race condition could create a situation where, without going through the checksum validation, data read from disks could be used for the reconstruction of data that failed to read due to disk errors.
The race condition only occurs when all the following conditions are true:

- The system is running IBM Storage Scale ECE or IBM Storage Scale System.
- The system is running these code levels: IBM Storage Scale 5.1.7.0 through 5.1.9.8 (IBM Storage Scale System 6.1.8.0 through 6.1.9.5) and IBM Storage Scale 5.2.0.0 through 5.2.2.0 (IBM Storage Scale System 6.2.0.0 through 6.2.2.0).
- nsdRAIDClientOnlyChecksum is enabled.
  Note: In recent IBM Storage Scale System configurations, the default is to have it enabled.
- Multiple threads are simultaneously performing full-track read operations to the same track.
- Disk errors or buffer trailer validation errors are affecting the reading of the corresponding strip data.

With these conditions, it is possible that data read from other strips will not be evaluated with the buffer checksum. Therefore, if there is silent data corruption within the buffer, it could be amplified to other areas in the same vtrack.
Users Affected:
This issue may affect clients that run IBM Storage Scale ECE or IBM Storage Scale System with the environment configuration parameter nsdRAIDClientOnlyChecksum enabled on the following versions of IBM Storage Scale:
IBM Storage Scale 5.1.7.0 through 5.1.9.8
(IBM Storage Scale System 6.1.8.0 through 6.1.9.5)
IBM Storage Scale 5.2.0.0 through 5.2.2.0
(IBM Storage Scale System 6.2.0.0 through 6.2.2.0)
Link

Storage alerts:

- **Vulnerabilities in the GUI affect IBM Storage Virtualise products and could allow authentication bypass and arbitrary code execution**

Vulnerabilities in the GUI affect IBM Storage Virtualise products and could allow authentication bypass and arbitrary code execution. The CLI is unaffected.
CVE-2025-0159 CVE-2025-0160.
Vulnerability Details
CVE-2025-0160 - IBM FlashSystems could allow a remote attacker with access to the system to execute arbitrary Java code due to improper restrictions in the RPCAdapter service.
CVE-2025-0159 - IBM FlashSystems could allow a remote attacker to bypass RPCAdapter endpoint authentication by sending a specifically crafted HTTP request.
Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Virtualize	8.5.0.0-8.5.0.13
IBM Storage Virtualize	8.5.1.0, 8.5.2.0-8.5.2.3, 8.5.3.0-8.5.3.1, 8.5.4.0
IBM Storage Virtualize	8.6.0.0-8.6.0.5
IBM Storage Virtualize	8.6.1.0, 8.6.2.0-8.6.2.1, 8.6.3.0
IBM Storage Virtualize	8.7.0.0-8.7.0.2
IBM Storage Virtualize	8.7.1.0, 8.7.2.0-8.7.2.1

Link

- **Possible false positive events on IBM Storage Scale System Storage Enclosures**

In MTM 5149-091 and MTM 5147-102, an IOM and its subcomponents may be reported as "not available" or "unknown", and a Call Home ticket may be opened. However, the reporting could be erroneous and the components may be working correctly. This can occur during the execution of the mmlsenclosure and mmhealth commands, when running gpfs.snap, or during an IBM Storage Scale System initiated a routine health check.
Users Affected

Users of either MTM 5149-091 or MTM 5147-102 on IBM Storage Scale System 6.1.9.5 (or earlier) or IBM Storage Scale System 6.2.2.0 (or earlier) firmware.

Problem Determination

In IBM Storage Scale System 6.1.9.5 (or earlier) or IBM Storage Scale System 6.2.2.0 (or earlier), the mmhealth command may report numerous failed sensor elements and may also indicate an absent IOM. A subsequent mmhealth command will show that these sensors are no longer failing.

Link

- **The following vulnerabilities can affect IBM Storage Scale System and IBM Storage Scale**

The following vulnerabilities can affect IBM Storage Scale System and IBM Storage Scale and could provide weaker than expected security are now fixed.

Vulnerability Details

CVE-2024-21235 - Vulnerability in Java SE (component: Hotspot). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to accessible data as well as unauthorized read access to a subset of accessible data.

CVE-2024-21217 - Vulnerability in Java SE (component: Serialization). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS).

CVE-2024-21210 - Vulnerability in Java SE (component: Hotspot). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some accessible data.

CVE-2024-21208 - Vulnerability in Java SE (component: Networking). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS).

CVE-2024-10917 - In Eclipse OpenJ9 versions up to 0.47, the JNI function GetStringUTFLength may return an incorrect value which has wrapped around. From 0.48 the value is correct but may be truncated to include a smaller number of characters.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale	5.1.9.7 and 5.2.2.0
IBM Storage Scale System	6.1.9.5 and 6.2.2.0

Link

Firmware updates:

- **New Microcode for Firmware 1060 ...1060.30**
  The latest service pack 1060.30 is now available for system firmware levels, ML1060, MM1060, and MH1060.
  Cross-reference information – Risk level: Informational

Product	Component	Platform	Version
IBM Power E1050 (9043-MRX)	Platform Independent		All Versions
IBM Power L1022 (9786-22H)	Platform Independent		All Versions
IBM Power L1024 (9786-42H)	Platform Independent		All Versions
IBM Power S1014 (9105-41B)	Platform Independent		All Versions
IBM Power S1022 (9105-22A)	Platform Independent		All Versions
IBM Power S1022s (9105-22B)	Platform Independent		All Versions
IBM Power S1024 (9105-42A)	Platform Independent		All Versions
IBM Power System S1012 (9028-21B)	Platform Independent		All Versions
Power System E1080 Server (9080-HEX)	Platform Independent		All Versions

  Link

Keep safe and hope to see you in Florida!
Red, Belisama