# March Newsletter

Subscribe/Unsubscribe

Greetings all,
Hope you are all keeping well.  A few interesting updates for March...

## A few updates to share

- Last month, Dino Quintero, Tim Simon and the editorial team published the PowerHA and VMRM updates.  This month it is great to see the update for the PowerHA Cookbook (See below).
- **Why IBM built an AI supercomputer in the cloud**.  An introduction to Vela, IBM's first AI-optimised, cloud-native supercomputer.
  Link
- Thank you Shawn Bodily for letting us know that there is an issue on VIOS 3.1.4.10, with the EN1K/EN1J 32Gbps SAN adapters, that prevents IBMi LPARs from seeing their boot disks.  This is a problem with the adapter firmware combined with VIOS level.  The current workaround is to use VIOS 3.1.3.x and support will be announcing an APAR soon.
- **IBM's Power10 chip and the on-processor accelerators for inferencing**  IBM was the pioneer in adding on-processor accelerators for inferencing in its IBM Power10 chip, called the Matrix Math Accelerator (MMA) engines. This gave the Power10 platform the ability to be faster than other hardware architectures without the need to spend an extra watt in energy with added GPUs.  The Power10 chip can extract insights from data faster than any other chip architecture and consumes much less energy than GPU-based systems.
  The data science libraries—such as openBLAS, libATen, Eigen and MLAS are already optimised to make use of the MMA engines.
  Link
- I have been fortunate to spend 3 days with Earl Jew looking at how AIX uses the features and architecture of the hardware, and how you should modify your LPARs as the generations of Power Hardware evolve.
  Many of Earl's presentations are available on the PowerVUG site.
  Link

## Quick bites

**Welcome for new and existing clients using IBM Storage Software products**
New and existing clients with an active support contract are being offered a free "Welcome Call", where they will be introduced to the local support team and be walked through the new support processes.  This includes:

- Spectrum Scale (formerly GPFS)
- Elastic Storage System (ESS)
- Spectrum Control / Storage Insights
- Spectrum Fusion

Link

**Using AIX 64K Active Memory Expansion with SAP**

AIX Active Memory Expansion (AME) is a feature that has been available for a quite a while in AIX.  AME uses the compression engine on the Power chip to compress memory without significantly impacting server performance, thus maintaining logical memory, but using less physical memory.  This whitepaper focuses on AME and its 64K page support when applied to SAP workload.  It contains the result of performance measurements with the SAP SD benchmark workload and gives general recommendations how to find optimal AME expansion factors.

Link

**What's next for IBM Power and SAP HANA**

Hard to believe it's already been over a year since IBM announced thier first IBM Power10 server, the Power E1080.  Now IBM has  announced some new enhancements to their IBM Power solutions designed to enable both our clients to optimise their Power server experience while simplifying and accelerating their journey to SAP HANA.

> **Accelerate SAP HANA migration with new 2-6TB bundles**
>
> The base of IBM customers using Power in larger SAP HANA workloads over 6TB is growing due to Power's outstanding performance, reliability and security. Power10 provides up to 2.5x better per core performance than the compared x86 servers so that customers have the option to do more with less.
>
> This offering is designed to meet the growing need for enterprise-class solutions for smaller SAP HANA workloads.  The options are either a Power L1022 or L1024 configured for smaller SAP HANA workloads.
>
> **Scale SAP HANA OLAP workloads with flexible options up to 40TB**
>
> IBM Power has a history of innovation and leadership for SAP HANA, allowing clients to create new SAP HANA environments flexibly by allocating incrementally from as low as 0.01 cores and 1GB memory.  SAP has just announced support for up to 40TB (OLAP only) on IBM Power, which makes it the first and only server vendor to be supported for SAP HANA workloads this large.

For more details, please contact your business partner.

Link

**IBM Electronic support gateway servers ip address changes**

IP addresses for IBM Electronic support gateway servers *eccgw01.boulder.ibm.com* and *eccgw02.rochester.ibm.co*m will be changing in 2023 as IBM migrates these servers to the Cloud.

Link

## In case you missed ….

- **ASEANZK AIX/IBM i/Linux on Power Meetup Group**

  At the March meeting, Simon Hutchinson (Mr. RPG) explained how building SQL Views should become a part of your development strategy and he give examples of the common ways he builds and uses Views to make his life and that of his team easier and simpler.  Why do the hard work yourself when something else can do it for you?

  Link

- **IBM PowerVUG**
  The March session covered FalconStor for Power and PowerVS
  Link

## Redbooks and Redpapers

- **IBM Power Systems Virtual Server Guide for IBM AIX and Linux** , Redbook, published on 23 March 2023
  Link
- **PowerHA SystemMirror for AIX Cookbook** , Draft Redbook, updated on 24 March 2023
  Link
- **Introduction to IBM PowerVM** , Redbook published 14 March 2023
  Link
- **Implementing, Tuning, and Optimizing Workloads with Red Hat OpenShift on IBM Power Systems** , draft Redbook, updated on 24 February 2023
  Link

## IBM alerts and notices

### AIX alerts:

- **AIX 7.3 TL0 PTFs in Error**
  APAR: IJ42793  Fix available in service pack: 7300-00-03-2246
  Users Affected:
  Systems running the 7300-00 Technology Level with any of the following filesets at or between the given levels:

  | MIN | MAX | FILESET |
  |---|---|---|
  | 7.3.0.1 | 7.3.0.1 | bos.rte.lvm |

  Problem description
  After having performed what seemed to be a successful restoration of AIX 7.3, the system hangs after reboot.
  Recommendation:
  Update to AIX 7300-00-03-2246 or later.
  Link
- **AIX 7.1 TL5 PTFs in Error**
  The following APARs are available in service pack: 7100-05-11-2246
  - IJ43085
  - IJ43017
  - IJ43102
  - IJ43095
  - IJ43097

  Link

- **AIX Service Pack 7300-00-03-224**
  Service Packs contain important fixes delivered between Technology Levels. This SP is based on Technology Level 7300-00.
  Link
- **AIX Service Pack 7100-05-11-2246**
  Service Packs contain important fixes delivered between Technology Levels. This SP is based on Technology Level 7100-05.
  Link

**Security Bulletins:**

- **CVE-2022-21426 may affect IBM® SDK, Java™ Technology Edition**
  CVE-2022-21426 was disclosed as part of the Oracle April 2022 Critical Patch Update.
  DESCRIPTION: An unspecified vulnerability in Java SE related to the JAXP component could allow an unauthenticated attacker to cause a denial of service resulting in a low availability impact using unknown attack vectors.
  Link
- **AIX and PowerVM Virtual I/O Server – Multiple vulnerabilities in OpenSSL**
  Vulnerabilities in OpenSSL could allow a remote attacker to cause a denial service (CVE-2022-3996, CVE-2023-0401, CVE-2022-4203, CVE-2023-0216, CVE-2023-0215, CVE-2023-0217, CVE-2023-0286, CVE-2022-4450) or obtain sensitive information (CVE-2022-4304). OpenSSL is used by AIX as part of AIX's secure network communications.
  Vulnerability Details
  - CVE-2022-3996: OpenSSL is vulnerable to a denial of service, caused by a double locking flaw when an X.509 certificate contains a malformed policy constraint and policy processing is enabled. By sending a specially-crafted request, a remote attacker could exploit this vulnerability to cause a denial of service condition on the web server.
    CVE-2023-0401: OpenSSL is vulnerable to a denial of service, caused by a NULL pointer dereference during PKCS7 data verification. A remote attacker could exploit this vulnerability to cause the application to crash.
    CVE-2022-4304: OpenSSL could allow a remote attacker to obtain sensitive information, caused by a timing-based side channel in the RSA Decryption implementation. By sending an overly large number of trial messages for decryption, an attacker could exploit this vulnerability to obtain sensitive information.
    CVE-2022-4203: OpenSSL is vulnerable to a denial of service, caused by a read buffer overrun triggered by the improper handling of X.509 certificate verification. A remote attacker could exploit this vulnerability to cause the system to crash.
    CVE-2023-0216: OpenSSL is vulnerable to a denial of service, caused by an invalid pointer dereference related to the incorrect handling of malformed

PKCS7 data. A remote attacker could exploit this vulnerability to cause the application to crash.
CVSS Base score: 7.5
CVE-2023-0215: OpenSSL is vulnerable to a denial of service, caused by a use-after-free error related to the incorrect handling of streaming ASN.1 data by the BIO_new_NDEF function. A remote attacker could exploit this vulnerability to cause a denial of service.
CVE-2023-0217: OpenSSL is vulnerable to a denial of service, caused by a NULL pointer dereference related to the validation of certain DSA public keys. A remote attacker could exploit this vulnerability to cause the application to crash.
CVE-2023-0286: OpenSSL is vulnerable to a denial of service, caused by a type confusion error related to X.400 address processing inside an X.509 GeneralName. By passing arbitrary pointers to a memcmp call, a remote attacker could exploit this vulnerability to read memory contents or cause a denial of service.
CVE-2022-4450: OpenSSL is vulnerable to a denial of service, caused by a double-free error related to the improper handling of specific PEM data by the PEM_read_bio_ex() function. By sending specially crafted PEM files for parsing, a remote attacker could exploit this vulnerability to cause the system to crash.

Affected product/version

| Affected Product(s) | Version(s) |
|---|---|
| AIX | 7.1 |
| AIX | 7.2 |
| AIX | 7.3 |
| VIOS | 3.1 |

The following fileset levels are vulnerable:

| Fileset | Lower Level | Upper Level |
|---|---|---|
| openssl.base | 1.0.2.500 | 1.0.2.2105 |
| openssl.base | 1.1.1.0 | 1.1.1.1202 |
| openssl.base | 1.1.2.0 | 1.1.2.1202 |
| openssl.base | 20.13.102.1000 | 20.16.102.2106 |
| openssl.base | 3.0.5.101 | 3.0.7.1000 |

Link

- **AIX and PowerVM Virtual I/O Server - AIX is vulnerable to denial of service vulnerabilities**

  UPDATED Mar 17 (Corrected the affected upper fileset levels for AIX 7.1 TL5 to show that SP11 is affected. Corrected the affected upper fileset levels for AIX 7.3 TL0 to show that SP03 is affected. Added iFixes for 7.1 TL5 SP10 and 7.3 TL0 SP03. The update applies to the kernel, perfstat, and pfcdd portions of the bulletin.)
  Vulnerabilities in the AIX kernel and kernel extensions could allow a non-privileged local user to cause a denial of service (CVE-2022-43380, CVE-2022-40233, CVE-2022-39165, CVE-2022-43848, CVE-2022-43849, CVE-2022-39164).

Vulnerability Details

CVE-2022-43380: IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX NFS kernel extension to cause a denial of service. IBM X-Force ID: 238640.

CVE-2022-40233: IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX TCP/IP kernel extension to cause a denial of service. IBM X-Force ID: 235599.

CVE-2022-39165: IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in CAA to cause a denial of service. IBM X-Force ID: 235183.

CVE-2022-43848: IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX perfstat kernel extension to cause a denial of service. IBM X-Force ID: 239169.

CVE-2022-43849: IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in the AIX pfcdd kernel extension to cause a denial of service. IBM X-Force ID: 239170.

CVE-2022-39164: IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in the AIX kernel to cause a denial of service. IBM X-Force ID: 235181.

Affected Products/Versions

| Affected Product(s) | Version(s) |
|---|---|
| AIX | 7.1 |
| AIX | 7.2 |
| AIX | 7.3 |
| VIOS | 3.1 |

Link

- **AIX is vulnerable to a denial of service due to lpd (CVE-2022-43382)**

UPDATED Mar 17 (Corrected the affected upper fileset levels for AIX 7.1 TL5 to show that SP11 is affected. Corrected the affected upper fileset levels for AIX 7.3 TL0 to show that SP03 is affected. Added iFixes for 7.1 TL5 SP10 and 7.3 TL0 SP03.) A vulnerability in the AIX lpd printer daemon could allow a local user with elevated privileges to cause a denial of service (CVE-2022-43382). The lpd daemon is the remote print server on AIX.

Vulnerability Details

CVE-2022-43382: IBM AIX could allow a local user with elevated privileges to exploit a vulnerability in the lpd daemon to cause a denial of service.

Affected Products/Versions

| Affected Product(s) | Version(s) |
|---|---|
| AIX | 7.1 |
| AIX | 7.2 |
| AIX | 7.3 |
| VIOS | 3.1 |

Link

### PowerSC alerts:

- **Multiple vulnerabilities in Curl affect PowerSC**

  There are multiple vulnerabilities in Curl that affect PowerSC.

  Vulnerability Details

  CVE-2022-42916: cURL libcurl could allow a remote attacker to obtain sensitive information, caused by a HSTS bypass flaw . By sending a specially-crafted URL with ASCII counterparts as part of the IDN conversion in host name, an attacker could exploit this vulnerability to obtain sensitive information from clear-text HTTP transmission, and use this information to launch further attacks against the affected system.

  CVE-2022-32221:L cURL libcurl could allow a remote attacker to bypass security restrictions, caused by a flaw when using the read callback (CURLOPT_READFUNCTION) to ask for data to send. By sending a specially-crafted request, an attacker could exploit this vulnerability to send wrong data or doing a use-after-free is not present in libcurl code.

  CVE-2022-35260: cURL libcurl is vulnerable to a denial of service, caused by a stack-based buffer overflow. By persuading a victim to open a specially-crafted netrc file, a remote attacker could exploit this vulnerability to cause a segfault, and results in a denial of service condition.

  CVE-2022-42915: cURL libcurl is vulnerable to a denial of service, caused by a double-free flaw in the error/cleanup handling. By sending a specially-crafted CONNECT request, a remote attacker could exploit this vulnerability to cause HTTP proxy to refuse the request, and results in a denial of service condition.

  Affected Product/Versions

  | Affected Product(s) | Version(s) |
  |---|---|
  | PowerSC | All |

  Link

### VIO Server updates:

- **VIOS 3.1.2.50**

  VIOS 3.1.2.50 Fix Pack is now available

  Link
- **VIOS 3.1.3.30**

  VIOS 3.1.3.30 Fix Pack is now available

  Link

### GPFS updates:

The following updates for Spectrum Scale are now available:

- **ESS_VM-6.1.6.0-x86_64-EMS**

  Link
- **ESS_DME_UNIFIED-6.1.6.0-x86_64-EMS**

  Link
- **ESS_DME_UNIFIED-6.1.6.0-ppc64LE-EMS**

Link

- **ESS_DAE_UNIFIED-6.1.6.0-ppc64LE-EMS**
  Link
- **ESS_DAE_UNIFIED-6.1.6.0-x86_64-EMS**
  Link
- **ESS_FIRMWARE-6.1.6.1-x86_64-Linux**
  Link
- **ESS_FIRMWARE-6.1.6.1-ppc64LE-Linux**
  Link

Keep safe and hope to catch up soon
Red, Belisama