Belisama

February Newsletter

Subscribe/Unsubscribe

Greetings all,
Wishing you the best for the Lunar New Year, Lent and Ramadan Mubara. I hope that you are able to spend time catching up with family.

A few updates to share

- Those of us that have been since the early days of AIX have grown comfortable, even complacent about creating mksysb's for our LPARs and our virtualisation layer – and assume that we will have NIM as a tool… But what about those with only a few LPARs, or new to the world of Power virtualisation without the luxury of AIX LPARs? Andrey addresses this in his latest blog: What should I do with my mksysb if I have no NIM? (Note this is his latest article on mksysb's, NIM and managing NIM with Ansbile)
  Link
- IBM consolidated Power announcements updated.
  Link
- Are you upgrading AIX 7.2 to 7.3? - Remember to run the dnf toolbox script to update dnf!
- AIX 7300-03-02-2546 is now available
  Link
- IBM Champion announcements coming soon – what this space!

Quick bites

AIX and VIO Server "Must Gather" for performance issues
Support has updated their "AIX MustGather: System Performance Analysis Product Documentation". Covers use of perfpmr, now to run and correct versions to download for AIX / VIOs – good tips on working with support to resolve issues quickly.
Link

New Microcode for firmware 1060 – Note: HIPER
The latest service pack 1060.61 is now available for system firmware levels, ML1060 and MM1060 and resolves this issue that was seen after some customers updated to 1060.60 and fixes a blank ASM screen when launched from the HMC.
Link

In case you missed ….

- **Welcome to IBM Support Customer Day**
  If you missed joining Support team looking at how IBM support is shifting from reactive to predictive / proactive, see the recording.
  Link

- **Power Systems VUG February 2026: IBM Spyre for Power**
  In the February session, Dr. Sebastian Lehrig, IBM's worldwide AI on Power Team Leader, spoke about Spyre. Follow the link for recordings and slides from this and previous meetings.
  Link

Redbooks and Redpapers

- **Zero Downtime, Automation, and Energy Optimization on IBM Power11**, Redbook, revised 20 February 2026
  Link
- **IBM i Migrate While Active**, Draft Redbook, published 19 February 2026
  Link
- **Implementing AI on Power11: Introducing the Spyre Adapter**, Draft Redbook, published 13 February 2026
  Link
- **Power11 Hybrid Cloud Solutions**, Draft Redbook, published 12 February 2026
  Link

IBM alerts and notices

AIX Notices:

- **IBM Power Maps updated - details**

Power10

- E1050 (9043-MRX) – All I/O
- E1050 (9043-MRX) – VIO only
- L1022 (9786-22H) – All I/O
- L1022 (9786-22H) – VIO only
- L1024 (9786-42H) – All I/O
- L1024 (9786-42H) – VIO only
- S1014 (9105-41B) - All I/O
- S1014 (9105-41B) – VIO only
- S1022 (9105-22A) – All I/O
- S1022 (9105-22A) – VIO only
- S1022s (9105-22B) – All I/O
- S1022s (9105-22B) – VIO only
- S1024 (9105-42A) – All I/O
- S1024 (9105-42A) – VIO only
- S1012 (9028-21B) – All I/O
- S1012 (9028-21B) – VIO only
- E1080 (9080-HEX) – All I/O
- E1080 (9080-HEX) – VIO only

Power9

- H922 (9223-22H) – All I/O

- H922 (9223-22H) – VIO only
- S914 (9009-41G) – All I/O
- S922 (9009-22A) – All I/O
- S922 (9009-22G) – All I/O
- S914 (9009-41A) – All I/O
- E950 (9040-MR9) – VIO only
- H924 (9223-42H) – All I/O
- H924 (9223-42H) – VIO only
- S924 (9009-42G) – All I/O
- S922 (9009-22G) – VIO only
- E950 (9040-MR9) – All I/O
- E980 (9080-M9S) - VIO only
- S914 (9009-41G) – VIO only
- S914 (9009-41A) – VIO only
- S924 (9009-42G) – VIO only
- S924 (9009-42A) – VIO only
- S922 (9009-22A) – VIO only
- E980 (9080-M9S) – All I/O
- S924 (9009-42A) – All I/O

Security Notices:

- **AIX Xorg X Server is vulnerable to memory corruption or a denial of service (CVE-2025-62230, CVE-2025-62231)**

  Updated Feb 24 2026: (New iFix for 7.3 TL3 SP2 provided with correct fileset prereqs. Updated the affected fileset levels to show that 7.3 TL3 SP2 is vulnerable.)
  Vulnerabilities in Xorg X Server could cause a memory corruption or denial of service (CVE-2025-62230, CVE-2025-62231).
  Vulnerability Details

  CVE-2025-62230 - A flaw was discovered in the X.Org X server's X Keyboard (Xkb) extension when handling client resource cleanup. The software frees certain data structures without properly detaching related resources, leading to a use-after-free condition. This can cause memory corruption or a crash when affected clients disconnect.
  CVE-2025-62231 - A flaw was identified in the X.Org X server's X Keyboard (Xkb) extension where improper bounds checking in the XkbSetCompatMap() function can cause an unsigned short overflow. If an attacker sends specially crafted input data, the value calculation may overflow, leading to memory corruption or a crash.

  Affected Products and Versions

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

The vulnerabilities in the following filesets are being addressed:

Fileset	Lower Level	Upper Level
X11.base.rte	7.2.5.0	7.2.5.201
X11.base.rte	7.3.0.0	7.3.0.0
X11.base.rte	7.3.3.0	7.3.3.1
X11.base.rte	7.3.4.0	7.3.4.0

Link

- **Multiple vulnerabilities impact AIX/VIOS due to ISC BIND (CVE-2025-40778, CVE-2025-40780, CVE-2025-8677)**

Vulnerabilities in ISC BIND could allow an attacker to inject forged data into the cache (CVE-2025-40778), predict the source port and query ID that BIND will use (CVE-2025-40780), or cause CPU exhaustion (CVE-2025-8677). AIX uses ISC BIND as as part of its DNS functions.

Vulnerability Details

CVE-2025-40778 - Under certain circumstances, BIND is too lenient when accepting records from answers, allowing an attacker to inject forged data into the cache. This issue affects BIND 9 versions 9.11.0 through 9.16.50, 9.18.0 through 9.18.39, 9.20.0 through 9.20.13, 9.21.0 through 9.21.12, 9.11.3-S1 through 9.16.50-S1, 9.18.11-S1 through 9.18.39-S1, and 9.20.9-S1 through 9.20.13-S1.

CVE-2025-40780 - In specific circumstances, due to a weakness in the Pseudo Random Number Generator (PRNG) that is used, it is possible for an attacker to predict the source port and query ID that BIND will use. This issue affects BIND 9 versions 9.16.0 through 9.16.50, 9.18.0 through 9.18.39, 9.20.0 through 9.20.13, 9.21.0 through 9.21.12, 9.16.8-S1 through 9.16.50-S1, 9.18.11-S1 through 9.18.39-S1, and 9.20.9-S1 through 9.20.13-S1.

CVE-2025-8677 - Querying for records within a specially crafted zone containing certain malformed DNSKEY records can lead to CPU exhaustion. This issue affects BIND 9 versions 9.18.0 through 9.18.39, 9.20.0 through 9.20.13, 9.21.0 through 9.21.12, 9.18.11-S1 through 9.18.39-S1, and 9.20.9-S1 through 9.20.13-S1.

Affected Products and Versions

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

The vulnerabilities are being addressed in the following filesets:

Fileset	Lower Level	Upper Level
bind.rte	7.1.916.0	7.1.916.4800
bind.rte	7.2.916.0	7.2.916.4801
bind.rte	7.2.918.0	7.2.918.2802
bind.rte	7.3.916.0	7.3.916.4800
bind.rte	7.3.918.0	7.3.918.2802

Link

AIX alerts:

- **AIX/VIOS is vulnerable to denial of service and possible code execution due to Perl (WS-2025-0004)**

  Vulnerability in Perl could allow an attacker to cause a denial of service or possibly execute code (WS-2025-0004). AIX uses Perl in various operating system components.

  Vulnerability Details

  WS-2025-0004 - Fix a class of false positives where input should have been rejected with error XML_ERROR_ASYNC_ENTITY; regression from CVE-2024-8176 fix pull request #973 (of Expat 2.7.0 and related backports). Please check the added unit tests for example documents.

  Affected Products and Versions

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

  The vulnerability is being addressed in the following fileset levels:

Fileset	Lower Level	Upper Level
perl.rte	5.34.0.0	5.34.1.8
perl.rte	5.38.0.0	5.38.2.3

  Link

AIX High Impact / Highly Pervasivealerts:

- **APAR IJ56896/IJ56918 LPAR may leak kernel memory, hang, or crash**

  AIX LPARs may leak kernel heap memory, hang, or crash.

  Risk categories

  System Outage

  Affected Domain

  AIX 7.2 : IJ56896

  AIX 7.3 : IJ56896/IJ56918

  Description

  These issues may occur during normal process scheduling with no specific trigger.

  They are more likely to be seen on 7.3 TL3 and later, on LPARs with multiple SRADs configured, while running workloads that have a lot of shared memory activity.

  Affected AIX Levels and Recommended Fixes

Minimum Affected	Maximum Affected	Fixing Level
AIX 7300-04	AIX 7300-04	AIX 7300-04-01
bos.mp64 7.3.4.0	bos.mp64 7.3.4.0	IJ57120
AIX 7300-03	AIX 7300-03-02-2546	AIX 7300-03-03
bos.mp64 7.3.3.0	bos.mp64 7.3.3.2	IJ56896

AIX 7300-02	AIX 7300-02-04-2520	N?A
bos.mp64 7.3.2.0	bos.mp64 7.3.2.5	
AIX 7200-05	AIX 7200-05-11-2546	AIX 7200-05-12
bos.mp64 7.2.5.0	bos.mp64 7.2.5.211	IJ57244

Link

PowerVC Security Bulletins:

- **qs parse module DoS vulnerability: arrayLimit bypass via bracket notation allows memory exhaustion (qs < 6.14.1)**

  An input validation flaw in qs < 6.14.1 allows attackers to bypass arrayLimit using bracket notation (a[]=x), leading to unauthenticated HTTP denial-of-service via memory exhaustion.

  Vulnerability Details

  CVE-2025-15284 - Improper Input Validation vulnerability in qs (parse modules) allows HTTP DoS.

  Affected Products and Versions

Affected Product(s)	Version(s)
PowerVC	2.2.1.2, 2.3.0, 2.3.1, 2.3.2

  Link

- **auth0/node-jws HS256 signature verification bypass via improper HMAC secret handling (≤3.2.2, 4.0.0)**

  auth0/node-jws HS256 signature verification bypass due to improper HMAC secret handling (versions ≤ 3.2.2 and 4.0.0)

  Vulnerability Details

  CVE-2025-65945 - auth0/node-jws is a JSON Web Signature implementation for Node.js. In versions 3.2.2 and earlier and version 4.0.0, auth0/node-jws has an improper signature verification vulnerability when using the HS256 algorithm under specific conditions. Applications are affected when they use the jws.createVerify() function for HMAC algorithms and use user-provided data from the JSON Web Signature protected header or payload in HMAC secret lookup routines, which can allow attackers to bypass signature verification. This issue has been patched in versions 3.2.3 and 4.0.1.

  Affected Products and Versions

Affected Product(s)	Version(s)
PowerVC	2.2.1.2, 2.3.0, 2.3.1, 2.3.2

  Link

HMC alerts:

- **Vulnerabilities in IBM Semeru SDK (CVE-2025-53057, CVE-2025-53066) affect Power HMC.**

  The IBM Semeru SDK is used by Power Hardware Management Console (HMC). HMC has addressed the applicable CVEs.

  Vulnerability Details

  CVE-2025-53057 - An unspecified vulnerability in Java SE related to the Security component could allow a remote attacker to cause no confidentiality impact, high integrity impact, and no availability impact.

  CVE-2025-53066 - An unspecified vulnerability in Java SE related to the JAXP component could allow a remote attacker to cause high confidentiality impact, no integrity impact, and no availability impact.

  Affected Products and Versions

Affected Product(s)	Version(s)
HMC	V10.3.1050.0 V10.3.1050.0
HMC	V11.1.1110.0 V11.1.1110.0

  Link

- **The openssh library is used by Power Hardware Management Console (HMC). HMC has addressed the applicable CVE.**
- Vulnerability Details

  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)
HMC	V10.3.1050.0 V10.3.1050.0
HMC	V11.1.1110.0 V11.1.1110.0

  Link

Keep safe and chat soon
Red, Belisama