Belisama

April Newsletter

Subscribe/Unsubscribe

Greetings all,
I hope that you all had a good May day and are busy getting your presentation ideas ready for TechXChange? Reminder: submissions close on 22/5.

A few updates to share

- Using dnf on AIX – easy, but managing repositories, not quite so simple. See Juraj's article on linkedin.
  Link
- IBM Community. Keep up to date with coming events:
  Link
- Had a bit of spare time over the last weekend and read some of the Power11 redbooks. It is worth getting down into the weeks as they do provide easy to understanding details about the design of the chip (particularly the Power11 scale out Redbook from last year) and the optimisation of memory and I/O.
- Support for SAP on E1180 2 node scale-out configurations with SMT8 has been announced.
  Link

Quick bites

AIX Performance Courses
Chris has just published a blog with details around the updated AIX courses. Link

SRIOV
Now a mature network virtualisation option. I have just been helping a colleague with some SRIOV questions, came across a few interesting articles on their configuration and use. In particular a useful one covering the labelling of ports for simplification, See Link

Capacity planning?
– do you use rperf?
If not you can download and run on your AIX server to calculate an estimated rPerf rating for that LPAR. For details see:
Link
(Also a reminder of the assumptions: Link)
To download: Link

Withdrawn products
Effective 31 July 2026 (or 30 July 2027 for China and South Korea), the following Machine type models are being withdrawn:

Description	Machine type	Model
Power E1050	9043	MRX
Power E1080	9080	HEX
Power S1022	9105	22A
Power S1022s	9105	22B
Power S1014	9105	41B
Power S1024	9105	42A
Power L1022	9786	22H
Power L1024	9786	42H

For details and other hardware see: Link

IBM Power Announcements for April

- IBM i Subscription: continued delivery of new offering structure for internal processing
- AIX and Availability Subscription Enhancements 2Q 2026
- Software withdrawal from marketing: AIX 2Q 2026
- IBM PowerVC introduces support for IBM Storage Policy-Based High Availability (PBHA) and IBM Storage Virtualize 9.1
- Power E1050 to E1150 conversion for 100GB DDR5 memory activation
- IBM i portfolio enhancements
- Hardware withdrawal: 4U DDIMM DDR4 Memory and miscellaneous features for selected Power servers
- IBM and Red Hat Enterprise Linux introduce a new Red Hat Enterprise Linux, and Red Hat OpenShift product structure on IBM Power servers
- IBM Support Line for Red Hat Products on IBM Power servers offers Remote Technical Support Services

Full list

In case you missed ….

- **Welcome to IBM Support Customer Day Q2 2026**
  This session covered the latest AI powered support capabilities, the enhanced IBM Customer Support Mobile App, and an overview of Advanced & Platinum support tiers.
  Link
- **AIX — The Future of Autonomous Infrastructure**.
  This event organised by Azucena Castro is a presentation by Jaqui Lynch.
  Link
- **Power Systems VUG April 2026**
  In this session, Tim Rowe introduces IBM Bob. IBM Bob is a software development AI assisted partner. Tim will cover what Bob is, how to access it, its benefits, and the best part, a live demo showing how Bob can be your development partner when it comes to

understanding your existing applications, as well as moving forward with modernisation! Taking your IBM i applications into the future.
Link

Redbooks and Redpapers

- **IBM Storage Scale System 6000 with NVIDIA DGX SuperPOD Deployment Guide**, Redpaper, published 09 April 2026
  Link

IBM alerts and notices

AIX alerts:

- **VPxxxx**
  Applies to:
  - Axx
    APAR: IJx

  Durinxxxted:

  USERS AFFECTED:

MIN	MAX	FILESET
7.1.5.39	7.1.5.44	bos.mp64
7.2.5.0	7.2.5.101	bos.mp64

- **Innnnn**
- **IJ123456:**

  Link

IBM alerts and notices

AIX alerts:

- **Vulnerability impacts AIX due to cURL libcurl (CVE-2025-14524)**
  Vulnerability in cURL libcurl might wrongly pass on an OAuth2 bearer token (CVE-2025-14524). AIX uses cURL libcurl as part of rsyslog, LV/PV encryption integration with HPCS and in Live Update for interacting with HMC.
  Vulnerability Details

  CVE-2025-14524 - When an OAuth2 bearer token is used for an HTTP(S) transfer, and that transfer performs a cross-protocol redirect to a second URL that uses an IMAP, LDAP, POP3 or SMTP scheme, curl might wrongly pass on the bearer token to the new target host.

  Affected Products and Versions

Affected Product(s)	Version(s)
AIX	7.3

  The following fileset levels are vulnerable:

Fileset	Lower Level	Upper Level
oss.lib.libcurl	7.79.1.0	7.79.1.0

oss.lib.libcurl	8.1.2.0	8.1.2.0
oss.lib.libcurl	8.5.0.0	8.5.0.2

Link

- **Multiple vulnerabilities in Python affect AIX**
  Vulnerabilities in Python could allow a null pointer dereference (CVE-2026-32776, CVE-2026-32778), an infinite loop (CVE-2026-32777), or impact availability (CVE-2025-12084). Python is used by AIX as part of Ansible node management automation.
  Vulnerability Details
  CVE-2026-32776 - libexpat before 2.7.5 allows a NULL pointer dereference with empty external parameter entity content.
  CVE-2026-32777 - libexpat before 2.7.5 allows an infinite loop while parsing DTD content.
  CVE-2026-32778 - libexpat before 2.7.5 allows a NULL pointer dereference in the function setContext on retry after an earlier ouf-of-memory condition.
  CWE: CWE-476: NULL Pointer Dereference
  CVE-2025-12084 - When building nested elements using xml.dom.minidom methods such as appendChild() that have a dependency on _clear_id_cache() the algorithm is quadratic. Availability can be impacted when building excessively nested documents.
  Affected Products and Versions

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

The vulnerabilities in the following filesets are being addressed:

Fileset	Lower Level	Upper Level
python3.9.base	3.9.0.0	3.9.23.0
python3.11.base	3.11.0.0	3.11.14.1

Link

AIX HIPER:

- **APAR IJ57286 IBM.SoftwareRM subsystem may kill all processes on an LPAR**
  IBM.SoftwareRM subsystem may kill all processes on an LPAR
  Risk categories
  System Outage
  Affected Domain
  All LPARs hosted on systems that are managed by an HMC connected to IBM’s Cloud Management Console (CMC), and that CMC is run as part of Power Enterprise Pools (PEP) 2.0.
  Description
  The RSCT subsystem, IBM.SoftwareRM, has a memory leak and will run out of memory after running for some time.

As the process approaches its memory limits, the error handling may result in unrelated processes on the LPAR getting killed.
This can only occur on systems that are managed by an HMC connected to IBM's Cloud Management Console (CMC), and that CMC is run as part of Power Enterprise Pools (PEP) 2.0.
We have typically seen this after IBM.SoftwareRM has been running for 2-3 months without restart.

Recommended Action

Download ifix

Link

- **SEA SHARING MODE NOT WORKING AFTER UPDATE TO 4.1.2.0**
  SEA with dedicated control channel VEA doesn't negotiate the sharing mode after update to 4.1.2
  Link

AIX Notices / How Tos:

- **PowerVM/VIOS FCA_ERR4/FCA_ERR12 errors on unused fibrechannel ports**
  Usually when there are unused ports on FC adapters, it is possible to disable those ports on the adapters and stop cfgdev/cfgmgr from configuring the devices, and this will stop all the error log messages.
  Objective

  Prevent "FCA_ERR12: 29FA8C20" and "FCA_ERR4: 7BFEEA1F" errors.
  This notices provides details to disable ports that are not connected and are intended to be not connected, if the errors are logged against ports that should be connected or should be in the "Available" status, you will need to troubleshoot those adapters accordingly.

  Symptoms;

  The below errors maybe found on errpt;

  LABEL: FCA_ERR12 IDENTIFIER: 29FA8C20
  LABEL: FCA_ERR4 IDENTIFIER: 7BFEEA1F

  Environment

  AIX
  PowerVM/VIOS
  AIX 7.2 TL5 with 32 GB/s FC NVMe adapters

  Link

PowerVM alerts:

- **Multiple vulnerabilities in PostgreSQL affect PowerVM VIOS**
  Vulnerabilities in PostgreSQL could allow an attacker to cause a denial of service (CVE-2025-4207), read sensitive data (CVE-2025-8713), or inject arbitrary code

(CVE-2025-8714, CVE-2025-8715). PowerVM VIOS uses PostgreSQL as part of Shared Storage Pools (SSP) and for internal administration purposes.

Vulnerability Details

CVE-2025-4207 - Buffer over-read in PostgreSQL GB18030 encoding validation allows a database input provider to achieve temporary denial of service on platforms where a 1-byte over-read can elicit process termination. This affects the database server and also libpq. Versions before PostgreSQL 17.5, 16.9, 15.13, 14.18, and 13.21 are affected.

CVE-2025-8713 - PostgreSQL optimiser statistics allow a user to read sampled data within a view that the user cannot access. Separately, statistics allow a user to read sampled data that a row security policy intended to hide. PostgreSQL maintains statistics for tables by sampling data available in columns; this data is consulted during the query planning process. Prior to this release, a user could craft a leaky operator that bypassed view access control lists (ACLs) and bypassed row security policies in partitioning or table inheritance hierarchies. Reachable statistics data notably included histograms and most-common-values lists. CVE-2017-7484 and CVE-2019-10130 intended to close this class of vulnerability, but this gap remained. Versions before PostgreSQL 17.6, 16.10, 15.14, 14.19, and 13.22 are affected.

CVE-2025-8714 - Untrusted data inclusion in pg_dump in PostgreSQL allows a malicious superuser of the origin server to inject arbitrary code for restore-time execution as the client operating system account running psql to restore the dump, via psql meta-commands. pg_dumpall is also affected. pg_restore is affected when used to generate a plain-format dump. This is similar to MySQL CVE-2024-21096. Versions before PostgreSQL 17.6, 16.10, 15.14, 14.19, and 13.22 are affected.

CVE-2025-8715 - Improper neutralization of newlines in pg_dump in PostgreSQL allows a user of the origin server to inject arbitrary code for restore-time execution as the client operating system account running psql to restore the dump, via psql meta-commands inside a purpose-crafted object name. The same attacks can achieve SQL injection as a superuser of the restore target server. pg_dumpall, pg_restore, and pg_upgrade are also affected. Versions before PostgreSQL 17.6, 16.10, 15.14, 14.19, and 13.22 are affected. Versions before 11.20 are unaffected. CVE-2012-0868 had fixed this class of problem, but version 11.20 reintroduced it.

Affected Products and Versions

Affected Product(s)	Version(s)
PowerVM VIOS	4.1.1
PowerVM VIOS	4.1.2

The vulnerability is being addressed in the following fileset levels:

Fileset	Lower Level	Upper Level
ios.database.rte	7.3.3.0	7.3.3.1
ios.viodb13.rte	7.3.4.0	7.3.4.0
ios.viodb15.rte	7.3.4.0	7.3.4.0

Link

- **GPFS/Scale alerts:**
- **IBM Storage Scale Software Version Recommendation Preventive Service Planning**
  IBM strongly recommends at least an annual upgrade of IBM Storage Scale code to stay at the recommended or latest levels of code as defined in the next tables.
  Definition:
  Extended Updated Support (EUS) releases are long term support releases on an 18 month cadence (nominally) that provides customers a stable release with ongoing PTFs (program temporary fixes) updates at typically 7-10 week intervals, which provides functionality and security fixes. See more details at IBM Storage Scale release philosophy.
  As announced in September 2024 on the Product Lifecycle pages, code editions for IBM Storage Scale 5.1.x (and its use on IBM Storage Scale System 6.1.x) reached End of Service (EOS) on September 30 of 2025.
  Link

Keep safe and hope that you have had the chance to “play” with some Power11 systems.
Red, Belisama