Belisama

July Newsletter

Subscribe/Unsubscribe

Greetings all,
Trust that you are all keeping well – and keeping up to date with the new Power11 announcements? Really looking forward to the deeper dives that are coming up – and of course the chance to learn more and catch up with the experts at TechXchange in Florida (only a few more months!).

A few updates to share

- For those on the Australian East Coast, hear from Bill Starke (Power Processor Lead Architect) what features are built into the new processor, and how they can help your organisation.
  - Sydney 5/8 1400-1700
    Register
  - Melbourne, 12/8 1400-1700
    Register
  - Brisbane, 14/8 1400-1700
    Register

  For those unable to attend, you will be able to download Bill's VUG session (see below).
- What is exciting about Power11? (Well, if you can join the above events to hear it from the horses mouth) – otherwise, the redbooks are out.
  At a high level, both the scale-out and scale-up systems have been announced, they look much the same as Power10, but have more cores – so initially will probably interest customers needing greater throughput as well as those on Power9 and below. Also if you are worried about your data centre footprint, maintenance costs or energy consumption, then they are well worth a look.
  Soon however we will be seeing more features becoming mainstream (see the Spyre card discussed last month).
- Andrey has been having some fun – have a look at the AI(x) assistant for AIX. Have a look at the Beta of the tool to help AIX administrators solve daily problems.
  Link
- The cost of a data breach – interesting but depressing reading
  Link
- Are you interested in training models? A note of warning, AI models may be passing hidden behaviours to each other, even if the training data appears benign.
  Link

Quick bites

TCP tuning for AIX systems
A summary of what basic TCP tuning are recommended to improve performance of WAN connections between AIX LPARs
Link

In case you missed ….

- **Power Systems VUG July 2025: Power11 with Bill Starke**
  Bill Starke, Distinguished Engineer: Power Processor Architect, talked about the generation of Power systems - Power11. This was the first of a series of sessions covering Power11 and focused on the processor/hardware of the new generation of systems.
  Link
  See the Power Systems VUG Wiki Site for past and future topics,
  Link

Coming soon

- **Power11 events**
  See above!

Redbooks and Redpapers

- **IBM i 7.6 features and function**, Redbook, 02 July 2025
  Link
- **IBM Power11 Scale-Out Servers: Introduction and Overview**, 19 July 2025, Draft Redbook
  Link
- **IBM Power Virtual Server Guide for IBM AIX and Linux**, 18 July 2025, Redbook
  Link
- **IBM Power11 E1150 Introduction and Technical Overview**, 12 July 2025, Draft Redbook
  Link
- **IBM Power E1180: Introduction and Overview**, 12 July 2025, Draft Redbook
  Link

IBM alerts and notices

AIX / PowerVM alerts:

- **Vulnerabilities in RPM could allow an attacker to execute arbitrary code (CVE-2025-3277, CVE-2025-29087) or cause a denial of service (CVE-2025-29088)**
  Vulnerabilities in RPM could allow an attacker to execute arbitrary code (CVE-2025-3277, CVE-2025-29087) or cause a denial of service (CVE-2025-29088). RPM is used by AIX for package management.

Vulnerability Details

CVE-2025-3277 - An integer overflow can be triggered in SQLite's `concat_ws()` function. The resulting, truncated integer is then used to allocate a buffer. When SQLite then writes the resulting string to the buffer, it uses the original, untruncated size and thus a wild Heap Buffer overflow of size ~4GB can be triggered. This can result in arbitrary code execution.
CVE-2025-29088 - In SQLite 3.49.0 before 3.49.1, certain argument values to sqlite3_db_config (in the C-language API) can cause a denial of service (application crash). An sz*nBig multiplication is not cast to a 64-bit integer, and consequently some memory allocations may be incorrect.
CVE-2025-29087 - In SQLite 3.44.0 through 3.49.0 before 3.49.1, the concat_ws() SQL function can cause memory to be written beyond the end of a malloc-allocated buffer. If the separator argument is attacker-controlled and has a large string (e.g., 2MB or more), an integer overflow occurs in calculating the size of the result buffer, and thus malloc may not allocate enough memory.

Affected Products and Versions

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

The vulnerabilities in the following filesets are being addressed:

Fileset	Lower Level	Upper Level
rpm.rte	4.15.1.1000	4.15.1.1015
rpm.rte	4.15.1.2000	4.15.1.2013
rpm.rte	4.18.1.2000	4.18.1.2005

Link

- **Vulnerabilities in libxml2 could cause a denial of service or other possible undefined behavior (CVE-2025-49796, CVE-2025-49794, CVE-2025-49795, CVE-2025-6021)**

Vulnerabilities in libxml2 could cause a denial of service or other possible undefined behavior (CVE-2025-49796, CVE-2025-49794, CVE-2025-49795, CVE-2025-6021). AIX uses libxml2 as part of its XML parsing functions.

Vulnerability Details

CVE-2025-49796 - A vulnerability was found in libxml2. Processing certain sch:name elements from the input XML file can trigger a memory corruption issue. This flaw allows an attacker to craft a malicious XML input file that can lead libxml to crash, resulting in a denial of service or other possible undefined behavior due to sensitive data being corrupted in memory.
CVE-2025-49794 - A use-after-free vulnerability was found in libxml2. This issue occurs when parsing XPath elements under certain circumstances when the XML schematron has the schema elements. This flaw allows a malicious

actor to craft a malicious XML document used as input for libxml, resulting in the program's crash using libxml or other possible undefined behaviors.
CVE-2025-49795 - A NULL pointer dereference vulnerability was found in libxml2 when processing XPath XML expressions. This flaw allows an attacker to craft a malicious XML input to libxml2, leading to a denial of service.
CVE-2025-6021 - A flaw was found in libxml2's xmlBuildQName function, where integer overflows in buffer size calculations can lead to a stack-based buffer overflow. This issue can result in memory corruption or a denial of service when processing crafted input.

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	7.2.5.205
bos.rte.control	7.3.1.0	7.3.1.3
bos.rte.control	7.3.2.0	7.3.2.3
bos.rte.control	7.3.3.0	7.3.3.1

Link

HMC alerts:

- **Vulnerabilities in libsoup library (CVE-2025-32050, CVE-2025-32052, CVE-2025-32053, CVE-2025-32906, CVE-2025-32911, CVE-2025-32913, CVE-2025-46420, CVE-2025-46421) affect Power HMC.**

  The libsoup library is used by Power Hardware Management Console (HMC). HMC has addressed the applicable CVEs.

  Vulnerability Details

  CVE-2025-32050 - A flaw was found in libsoup. The libsoup append_param_quoted() function may contain an overflow bug resulting in a buffer under-read.
  CVE-2025-32052 - A flaw was found in libsoup. A vulnerability in the sniff_unknown() function may lead to heap buffer over-read.
  CVE-2025-32053 - A flaw was found in libsoup. A vulnerability in sniff_feed_or_html() and skip_insignificant_space() functions may lead to a heap buffer over-read.
  CVE-2025-32906 - A flaw was found in libsoup, where the soup_headers_parse_request() function may be vulnerable to an out-of-bound read. This flaw allows a malicious user to use a specially crafted HTTP request to crash the HTTP server.

CVE-2025-32911 - A use-after-free type vulnerability was found in libsoup, in the soup_message_headers_get_content_disposition() function. This flaw allows a malicious HTTP client to cause memory corruption in the libsoup server.
CVE-2025-32913 - A flaw was found in libsoup, where the soup_message_headers_get_content_disposition() function is vulnerable to a NULL pointer dereference. This flaw allows a malicious HTTP peer to crash a libsoup client or server that uses this function.
CVE-2025-46420 - A flaw was found in libsoup. It is vulnerable to memory leaks in the soup_header_parse_quality_list() function when parsing a quality list that contains elements with all zeroes.
CVE-2025-46421 - A flaw was found in libsoup. When libsoup clients encounter an HTTP redirect, they mistakenly send the HTTP Authorisation header to the new host that the redirection points to. This allows the new host to impersonate the user to the original host that issued the redirect.

Affected Products and Versions

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

Link

- **Vulnerability in expat library (CVE-2024-8176) affects Power HMC.**

The expat library is used by Power Hardware Management Console (HMC). HMC has addressed the applicable CVE.

Vulnerability Details

CVE-2024-8176 - A stack overflow vulnerability exists in the libexpat library due to the way it handles recursive entity expansion in XML documents. When parsing an XML document with deeply nested entity references, libexpat can be forced to recurse indefinitely, exhausting the stack space and causing a crash. This issue could lead to denial of service (DoS) or, in some cases, exploitable memory corruption, depending on the environment and library usage.
CVE-2025-21587 - An unspecified vulnerability in Java SE related to the Server: DDL component could allow a remote attacker to cause high confidentiality and high integrity impact.
CVE-2025-30698 - An unspecified vulnerability in Java SE related to the 2D component could allow a remote attacker to cause low confidentiality, low integrity and low availability impact.
CVE-2025-2900 - IBM Semeru Runtime 8.0.302.0 through 8.0.442.0, 11.0.12.0 through 11.0.26.0, 17.0.0.0 through 17.0.14.0, and 21.0.0.0 through 12.0.6.0 is vulnerable to a denial of service caused by a buffer overflow and subsequent crash, due to a defect in its native AES/CBC encryption implementation.
CVE-2024-56171- libxml2 before 2.12.10 and 2.13.x before 2.13.6 has a use-after-free in xmlSchemaIDCFillNodeTables and

xmlSchemaBubbleIDCNodeTables in xmlschemas.c. To exploit this, a crafted XML document must be validated against an XML schema with certain identity constraints, or a crafted XML schema must be used.
CVE-2025-24928 - libxml2 before 2.12.10 and 2.13.x before 2.13.6 has a stack-based buffer overflow in xmlSnprintfElements in valid.c. To exploit this, DTD validation must occur for an untrusted document or untrusted DTD. NOTE: this is similar to CVE-2017-9047.
CVE-2025-27363 - An out of bounds write exists in FreeType versions 2.13.0 and below (newer versions of FreeType are not vulnerable) when attempting to parse font subglyph structures related to TrueType GX and variable font files. The vulnerable code assigns a signed short value to an unsigned long and then adds a static value causing it to wrap around and allocate too small of a heap buffer. The code then writes up to 6 signed long integers out of bounds relative to this buffer. This may result in arbitrary code execution. This vulnerability may have been exploited in the wild.

Affected Products and Versions

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

Link

PowerVC alerts:

- **A number of security bulletins have been published for PowerVC**
  - OTP vulnerabilty
  - Unauthorised network tag modification
  - SSRF vulnerability
  - Jackson-Core stack overflow
  - ACE vulnerability
  - SSL vulnerability

GPFS/Scale HIPERs:

- **Potential undetected data corruption in IBM Storage Scale when compressed snapshot files are read and the highly-available write cache (HAWC) feature is enabled causing unexpected data reads**

IBM has identified a problem with reading compressed snapshot files when the highly-available write cache (HAWC) feature is enabled. This can cause transient, unexpected data reads from snapshot files.

Recommended Action

Support for the HAWC feature is being discontinued. Clients should disable HAWC by setting the writeCacheThreshold file system configuration value to 0. To apply this setting, run the following command:

mmchfs Device --write-cache-threshold 0

Note: that disabling the HAWC feature may lead to measurable performance degradation for certain workloads on file systems where the feature was previously enabled.
Further details in Stabilised, deprecated, and discontinued features in IBM Storage Scale.

Link

- **IBM Storage Scale 5.1.0.0 - 5.2.2.1: Potential risk of reading stale or uninitialised data while the mmchdisk start command is being executed on replicated file systems**

In IBM Storage Scale versions 5.1.0.0 through 5.2.2.1 (IBM Storage Scale System 6.1.0.0 through 6.2.2.1), IBM has identified a potential integrity issue for file system data. Under certain conditions, incorrect snapshot data —either stale or uninitialised- might be read while the mmchdisk start command is being executed on file systems with replication enabled

Description

The mmchdisk start command is used to bring disks in the down state back to the up state. In replicated file systems, this command also attempts to repair stale data on these disks. If a replica on a down disk is not written during a file block update, that replica may become stale or remain uninitialized until the completion of the mmchdisk start command, which fixes the situation. Stale replicas are not read by applications.
After the mmchdisk start is issued, the affected disks enter an unrecovered state. Upon successful completion of the command, these disks transition back to the up state, and all replicas become readable by applications again.
Tip: The mmlsdisk command can be used to check disk states. Any disk in the unrecovered state gets listed in the output.
If a workload accesses the snapshot data while a disk remains in the unrecovered state, a problem has been uncovered where there is a risk of reading stale or uninitialized data —if the affected disks have not yet been repaired.

Users affected

Customers that run IBM Storage Scale versions 5.1.0.0 through 5.2.2.1 (IBM Storage Scale 6.1.0.0 through 6.2.2.1), particularly if they are accessing snapshot data while the mmchdisk start command is in progress.
This issue may occur when replication is enabled for user data, metadata, or both.

Recommended Action

To avoid this issue, take the following action:
Upgrade all nodes to IBM Storage Scale version 5.2.3.0 (IBM Storage Scale System 6.2.3.0) or later

Link

GPFS/Scale alerts/flashes:

- **IBM Storage Scale versions 5.2.3.0 and 5.2.3.1 are affected by a security vulnerability that can allow unauthorised access to user files (CVE-2025-36104)**

  IBM has identified a data access problem in IBM Storage Scale 5.2.3.0 and 5.2.3.1 regarding the SMB protocol and acccess control lists (ACLs). The problem occurs with the use of inherited ACLs on directories or files that are created or modified through the SMB protocol. A fix for this vulnerability is available.

  Vulnerability Details

  CVE-2025-36104 - IBM Storage Scale could allow an authenticated user to obtain sensitive information from files due to the insecure permissions inherited through the SMB protocol.

  Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale	5.2.3.0 - 5.2.3.1

  Link

- **Potential access or permission denied error with NFSv4 during a ‘git clone’ or ‘file open’ operation after an upgrade to IBM Storage Scale 5.1.9.10, 5.2.3.0, or 5.2.3.1**

  IBM has identified a potential issue with NFSv4 file access that may occur after an upgrade in environments that use IBM Storage Scale Cluster Export Services Network File System (CES NFS). This issue has been observed especially with NFSv4 mounts that use NFSv4.0, NFSv4.1, or NFSv4.2.

  Content

  After an upgrade to IBM Storage Scale version 5.1.9.10, 5.2.3.0, or 5.2.3.1, clients that access files over NFSv4 may see access problems or "permission denied" errors. A common case when this issue can happen is when a user tries to run git clone into a directory mounted over NFS.

  Link

- **The following vulnerabilities that can affect IBM Storage Scale System are now included in 6.2.2.1 and 6.1.9.6.**

  The following vulnerabilities that can affect IBM Storage Scale System and could provide weaker than expected security are now fixed in 6.2.2.1 and 6.1.9.6.

  CVE-2024-42240 - In the Linux kernel, the following vulnerability has been resolved: x86/bhi: Avoid warning in #DB handler due to BHI mitigation When BHI mitigation is enabled, if SYSENTER is invoked with the TF flag set then entry_SYSENTER_compat() uses CLEAR_BRANCH_HISTORY and calls the clear_bhb_loop() before the TF flag is cleared. This causes the #DB handler (exc_debug_kernel()) to issue a warning because single-step is used outside the entry_SYSENTER_compat() function. To address this issue,

entry_SYSENTER_compat() should use CLEAR_BRANCH_HISTORY after making sure the TF flag is cleared. The problem can be reproduced with the following sequence:

```
$ cat sysenter_step.c int main() { asm("pushf; pop %ax; bts $8,%ax; push %ax; popf; sysenter"); } $ gcc -o sysenter_step sysenter_step.c $ ./sysenter_step Segmentation fault (core dumped) The program is expected to crash, and the #DB handler will issue a warning. Kernel log: WARNING: CPU: 27 PID: 7000 at arch/x86/kernel/traps.c:1009 exc_debug_kernel+0xd2/0x160 ... RIP: 0010:exc_debug_kernel+0xd2/0x160 ... Call Trace: <#DB> ? show_regs+0x68/0x80 ? __warn+0x8c/0x140 ? exc_debug_kernel+0xd2/0x160 ? report_bug+0x175/0x1a0 ? handle_bug+0x44/0x90 ? exc_invalid_op+0x1c/0x70 ? asm_exc_invalid_op+0x1f/0x30 ? exc_debug_kernel+0xd2/0x160 exc_debug+0x43/0x50 asm_exc_debug+0x1e/0x40 RIP: 0010:clear_bhb_loop+0x0/0xb0 ... </#DB> ? entry_SYSENTER_compat_after_hwframe+0x6e/0x8d [ bp: Massage commit message. ]
```

CVE-2024-26906 - In the Linux kernel, the following vulnerability has been resolved: x86/mm: Disallow vsyscall page read for copy_from_kernel_nofault() When trying to use copy_from_kernel_nofault() to read vsyscall page through a bpf program, the following oops was reported: BUG: unable to handle page fault for address: ffffffffff600000 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 3231067 P4D 3231067 PUD 3233067 PMD 3235067 PTE 0 Oops: 0000 [#1] PREEMPT SMP PTI CPU: 1 PID: 20390 Comm: test_progs ..... 6.7.0+ #58 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996) ..... RIP: 0010:copy_from_kernel_nofault+0x6f/0x110 ..... Call Trace: ? copy_from_kernel_nofault+0x6f/0x110 bpf_probe_read_kernel+0x1d/0x50 bpf_prog_2061065e56845f08_do_probe_read+0x51/0x8d trace_call_bpf+0xc5/0x1c0 perf_call_bpf_enter.isra.0+0x69/0xb0 perf_syscall_enter+0x13e/0x200 syscall_trace_enter+0x188/0x1c0 do_syscall_64+0xb5/0xe0 entry_SYSCALL_64_after_hwframe+0x6e/0x76 ..... ---[end trace 0000000000000000]--- The oops is triggered when: 1) A bpf program uses bpf_probe_read_kernel() to read from the vsyscall page and invokes copy_from_kernel_nofault() which in turn calls __get_user_asm(). 2) Because the vsyscall page address is not readable from kernel space, a page fault exception is triggered accordingly. 3) handle_page_fault() considers the vsyscall page address as a user space address instead of a kernel space

address. This results in the fix-up setup by bpf not being applied and a page_fault_oops() is invoked due to SMAP. Considering handle_page_fault() has already considered the vsyscall page address as a userspace address, fix the problem by disallowing vsyscall page read for copy_from_kernel_nofault().
CVE-2024-40997 - In the Linux kernel, the following vulnerability has been resolved: cpufreq: amd-pstate: fix memory leak on CPU EPP exit The cpudata memory from kzalloc() in amd_pstate_epp_cpu_init() is not freed in the analogous exit function, so fix that. [rjw: Subject and changelog edits]
CVE-2024-34064 - Jinja is an extensible templating engine. The `xmlattr` filter in affected versions of Jinja accepts keys containing non-attribute characters. XML/HTML attributes cannot contain spaces, `/`, `>`, or `=`, as each would then be interpreted as starting a separate attribute. If an application accepts keys (as opposed to only values) as user input, and renders these in pages that other users see as well, an attacker could use this to inject other attributes and perform XSS. The fix for CVE-2024-22195 only addressed spaces but not other characters. Accepting keys as user input is now explicitly considered an unintended use case of the `xmlattr` filter, and code that does so without otherwise validating the input should be flagged as insecure, regardless of Jinja version. Accepting _values_ as user input continues to be safe. This vulnerability is fixed in 3.1.4.
Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale System	6.2.0.0 - 6.2.2.0
IBM Storage Scale System	6.1.0.0 - 6.1.9.5

Link

GPFS / Scale downloads and drivres:

- **Potential access loss for SMB CES users**
  Microsoft Windows Server update CVE-2025-49716 disables an API that is used by Storage Scale Cluster Export Services (CES) SMB (Samba Winbind).
  Without the API, users can no longer connect to SMB shares served from Storage Scale CES SMB, specifically when idmap-information is stored in Active Directory.
  Link

Keep safe and hope to catch up at one of the Power11 events.
Red, Belisama