Belisama

March Newsletter

Subscribe/Unsubscribe

Greetings all,
I hope that you all had a good break over Easter – and for those that celebrate - a joyful Eid.

A few updates to share

- You are probably aware of Hashicorp, and that it is now part of IBM. I had hoped that this would fix the problem of Terraform support for Power, PowerVM, HMC, etc. Sadly there is still no mention of ppc64le on the Hashicorp site or in their archive. However you will still be able to find some old code/providers/GitHub projects for IBM Power (eg: Link). Let's see if we can encourage this to change!
- IBM has announced the champions for '26 – congratulations to all the new members and welcome back to the existing champions!
  On a personal note, Thank you IBM and the Champion team for allowing me again to take part in this programme, and for all the support you provide.
- IBM TechXChange Atlanta
  Be a speaker at IBM TechXchange 2026 Atlanta, GA | Oct. 26–29! Submit your proposal by May 22.
  Link
- In the last month, I have seen some "performance" issues in a variety of different scenarios – all of which had a common cause. Don't forget the impact that a failure or delay in name resolution can cause – so remember to check your hosts file for critical hosts – and edit your netsvc.conf file (AIX) or nsswitch.conf (Linux). If you don't have control over the DNS, don't subject your critical systems to it's vagaries.

Quick bites

Want to use rsyslog rather than the native AIX syslog??
IBM support has published the steps to download and install `rsyslog` on your AIX LPAR.
Link

Issues with dnf on AIX?
It is likely that you will need to upgrade python on your system. Currently the AIX toolbox python3 is based on python3.9 – support for which ended on the 31/10/25. It is recommended that you download and install python3.12 which is now available – and you should see modules built on python3.12 uploaded soon.
There is a good blog covering this - Link

In case you missed ….

- **March PowerVUG**
  Jaqui Lynch on top tips for successful administration of your VIO servers.
  The move to artificial intelligence and cloud requires a fully automated virtualised environment to be successful. VIO servers are a critical component of your POWER system setup. If they are not happy then no client LPAR will be happy.
  This session provides tips on setting up and maintaining VIO servers including upgrades and patching and will also cover upgrading to V4 with tips provided from the latest HMC version and its interactions with the VIO server(s).
  Session Materials

Coming soon

- **Support Customer Day Q2 2026**
  15/4/26 15:30 AEST; 13:30 SGT This is the second Customer day for ‘26 – with sessions with IBM Support leadership, architects, and subject-matter experts showcasing latest technologies. Deep dives into client facing AI-driven capabilities and the mobile application. Support offerings that meet your needs.
  Link
- **Power Systems VUG April 2026: Meet IBM Bob with Tim Rowe**
  In this months VUG, Tim Rowe will introduce IBM Bob - 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.

Redbooks and Redpapers

- **Implementing AI on Power11: Introducing the IBM Spyre Accelerator**, Redbook, 31 March 2026
  Link
- **IBM Storage Scale System Introduction Guide**, Redpaper, 28 March 2026
  Link
- **Setting Up IBM Storage Scale with NVIDIA Base Command Manager**, Redbook Experience (!?!), 27 March 2026
  Link
- **Implementation Guide for IBM Storage Scale System 6000**, Redbook, 26 March 2026
  Link
- **Security and Cyber Resilience with IBM Power11**, Redbook, 20 March 2026
  Link
- **High Availability and Disaster Recovery Solutions on IBM Power Virtual Server**, Draft Redbook, 06 March 2026
  Link

IBM alerts and notices

AIX/PowerVM alerts:

- **Security Bulletin: AIX/VIOS Python is vulnerable to a null pointer dereference**
  Vulnerabilities in Python could cause a null pointer dereference (CVE-2026-24515) or an integer overflow (CVE-2026-25210). Python is used by AIX as part of Ansible node management automation.
  Vulnerability Details
  CVE-2026-24515 - In libexpat before 2.7.4, XML_ExternalEntityParserCreate does not copy unknown encoding handler user data.
  CVE-2026-25210 - In libexpat before 2.7.4, the doContent function does not properly determine the buffer size bufSize because there is no integer overflow check for tag buffer reallocation.
  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	3.9.24.0
python3.11.base	3.11.0.0	3.11.14.0

  Link

- **Vulnerabilities in OpenSSL could allow an attacker to potentially execute arbitrary code or cause a denial of service. OpenSSL is used by AIX as part of AIX's secure network communications.**
  Vulnerability Details
  CVE-2025-15467 - Issue summary: Parsing CMS AuthEnvelopedData or EnvelopedData message with maliciously crafted AEAD parameters can trigger a stack buffer overflow. Impact summary: A stack buffer overflow may lead to a crash, causing Denial of Service, or potentially remote code execution. When parsing CMS (Auth)EnvelopedData structures that use AEAD ciphers such as AES-GCM, the IV (Initialization Vector) encoded in the ASN.1 parameters is copied into a fixed-size stack buffer without verifying that its length fits the destination. An attacker can supply a crafted CMS message with an oversized IV, causing a stack-based out-of-bounds write before any authentication or tag verification occurs. Applications and services that parse untrusted CMS or PKCS#7 content using AEAD ciphers (e.g., S/MIME (Auth)EnvelopedData with AES-GCM) are vulnerable. Because the overflow occurs prior to authentication, no valid key material is required to trigger it. While exploitability to remote code execution depends on platform and

toolchain mitigations, the stack-based write primitive represents a severe risk. The FIPS modules in 3.6, 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the CMS implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4, 3.3 and 3.0 are vulnerable to this issue. OpenSSL 1.1.1 and 1.0.2 are not affected by this issue.

CVE-2025-68160 - Issue summary: Writing large, newline-free data into a BIO chain using the line-buffering filter where the next BIO performs short writes can trigger a heap-based out-of-bounds write. Impact summary: This out-of-bounds write can cause memory corruption which typically results in a crash, leading to Denial of Service for an application. The line-buffering BIO filter (BIO_f_linebuffer) is not used by default in TLS/SSL data paths. In OpenSSL command-line applications, it is typically only pushed onto stdout/stderr on VMS systems. Third-party applications that explicitly use this filter with a BIO chain that can short-write and that write large, newline-free data influenced by an attacker would be affected. However, the circumstances where this could happen are unlikely to be under attacker control, and BIO_f_linebuffer is unlikely to be handling non-curated data controlled by an attacker. For that reason the issue was assessed as Low severity. The FIPS modules in 3.6, 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the BIO implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4, 3.3, 3.0, 1.1.1 and 1.0.2 are vulnerable to this issue.

CVE-2025-69418 - Issue summary: When using the low-level OCB API directly with AES-NI orbrother hardware-accelerated code paths, inputs whose length is not a multiplebrof 16 bytes can leave the final partial block unencrypted and unauthenticated.brbrImpact summary: The trailing 1-15 bytes of a message may be exposed inbrcleartext on encryption and are not covered by the authentication tag,brallowing an attacker to read or tamper with those bytes without detection.brbrThe low-level OCB encrypt and decrypt routines in the hardware-acceleratedbrstream path process full 16-byte blocks but do not advance the input/outputbrpointers. The subsequent tail-handling code then operates on the originalbrbase pointers, effectively reprocessing the beginning of the buffer whilebrleaving the actual trailing bytes unprocessed. The authentication checksumbralso excludes the true tail bytes.brbrHowever, typical OpenSSL consumers using EVP are not affected because thebrhigher-level EVP and provider OCB implementations split inputs so that fullbrblocks and trailing partial blocks are processed in separate calls, avoidingbrthe problematic code path. Additionally, TLS does not use OCB ciphersuites.brThe vulnerability only affects

applications that call the low-levelbrCRYPTO_ocb128_encrypt() or CRYPTO_ocb128_decrypt() functions directly withbrnon-block-aligned lengths in a single call on hardware-accelerated builds.brFor these reasons the issue was assessed as Low severity.brbrThe FIPS modules in 3.6, 3.5, 3.4, 3.3, 3.2, 3.1 and 3.0 are not affectedbrby this issue, as OCB mode is not a FIPS-approved algorithm.brbrOpenSSL 3.6, 3.5, 3.4, 3.3, 3.0 and 1.1.1 are vulnerable to this issue.brbrOpenSSL 1.0.2 is not affected by this issue.

CVE-2025-69419 - Issue summary: Calling PKCS12_get_friendlyname() function on a maliciously crafted PKCS#12 file with a BMPString (UTF-16BE) friendly name containing non-ASCII BMP code point can trigger a one byte write before the allocated buffer. Impact summary: The out-of-bounds write can cause a memory corruption which can have various consequences including a Denial of Service. The OPENSSL_uni2utf8() function performs a two-pass conversion of a PKCS#12 BMPString (UTF-16BE) to UTF-8. In the second pass, when emitting UTF-8 bytes, the helper function bmp_to_utf8() incorrectly forwards the remaining UTF-16 source byte count as the destination buffer capacity to UTF8_putc(). For BMP code points above U+07FF, UTF-8 requires three bytes, but the forwarded capacity can be just two bytes. UTF8_putc() then returns -1, and this negative value is added to the output length without validation, causing the length to become negative. The subsequent trailing NUL byte is then written at a negative offset, causing write outside of heap allocated buffer. The vulnerability is reachable via the public PKCS12_get_friendlyname() API when parsing attacker-controlled PKCS#12 files. While PKCS12_parse() uses a different code path that avoids this issue, PKCS12_get_friendlyname() directly invokes the vulnerable function. Exploitation requires an attacker to provide a malicious PKCS#12 file to be parsed by the application and the attacker can just trigger a one zero byte write before the allocated buffer. For that reason the issue was assessed as Low severity according to our Security Policy. The FIPS modules in 3.6, 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the PKCS#12 implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4, 3.3, 3.0 and 1.1.1 are vulnerable to this issue. OpenSSL 1.0.2 is not affected by this issue.

CVE-2025-69420 -Issue summary: A type confusion vulnerability exists in the TimeStamp Response verification code where an ASN1_TYPE union member is accessed without first validating the type, causing an invalid or NULL pointer dereference when processing a malformed TimeStamp Response file. Impact summary: An application calling TS_RESP_verify_response() with a malformed TimeStamp Response can be caused to dereference an invalid or

NULL pointer when reading, resulting in a Denial of Service. The functions ossl_ess_get_signing_cert() and ossl_ess_get_signing_cert_v2() access the signing cert attribute value without validating its type. When the type is not V_ASN1_SEQUENCE, this results in accessing invalid memory through the ASN1_TYPE union, causing a crash. Exploiting this vulnerability requires an attacker to provide a malformed TimeStamp Response to an application that verifies timestamp responses. The TimeStamp protocol (RFC 3161) is not widely used and the impact of the exploit is just a Denial of Service. For these reasons the issue was assessed as Low severity. The FIPS modules in 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the TimeStamp Response implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4, 3.3, 3.0 and 1.1.1 are vulnerable to this issue. OpenSSL 1.0.2 is not affected by this issue.

CVE-2025-69421 - Issue summary: Processing a malformed PKCS#12 file can trigger a NULL pointer dereference in the PKCS12_item_decrypt_d2i_ex() function. Impact summary: A NULL pointer dereference can trigger a crash which leads to Denial of Service for an application processing PKCS#12 files. The PKCS12_item_decrypt_d2i_ex() function does not check whether the oct parameter is NULL before dereferencing it. When called from PKCS12_unpack_p7encdata() with a malformed PKCS#12 file, this parameter can be NULL, causing a crash. The vulnerability is limited to Denial of Service and cannot be escalated to achieve code execution or memory disclosure. Exploiting this issue requires an attacker to provide a malformed PKCS#12 file to an application that processes it. For that reason the issue was assessed as Low severity according to our Security Policy. The FIPS modules in 3.6, 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the PKCS#12 implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4, 3.3, 3.0, 1.1.1 and 1.0.2 are vulnerable to this issue.

CVE-2026-22795 - Issue summary: An invalid or NULL pointer dereference can happen in an application processing a malformed PKCS#12 file. Impact summary: An application processing a malformed PKCS#12 file can be caused to dereference an invalid or NULL pointer on memory read, resulting in a Denial of Service. A type confusion vulnerability exists in PKCS#12 parsing code where an ASN1_TYPE union member is accessed without first validating the type, causing an invalid pointer read. The location is constrained to a 1-byte address space, meaning any attempted pointer manipulation can only target addresses between 0x00 and 0xFF. This range corresponds to the zero page, which is unmapped on most modern operating systems

and will reliably result in a crash, leading only to a Denial of Service. Exploiting this issue also requires a user or application to process a maliciously crafted PKCS#12 file. It is uncommon to accept untrusted PKCS#12 files in applications as they are usually used to store private keys which are trusted by definition. For these reasons, the issue was assessed as Low severity. The FIPS modules in 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the PKCS12 implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4, 3.3, 3.0 and 1.1.1 are vulnerable to this issue. OpenSSL 1.0.2 is not affected by this issue.

CVE-2026-22796- Issue summary: A type confusion vulnerability exists in the signature verification of signed PKCS#7 data where an ASN1_TYPE union member is accessed without first validating the type, causing an invalid or NULL pointer dereference when processing malformed PKCS#7 data. Impact summary: An application performing signature verification of PKCS#7 data or calling directly the PKCS7_digest_from_attributes() function can be caused to dereference an invalid or NULL pointer when reading, resulting in a Denial of Service. The function PKCS7_digest_from_attributes() accesses the message digest attribute value without validating its type. When the type is not V_ASN1_OCTET_STRING, this results in accessing invalid memory through the ASN1_TYPE union, causing a crash. Exploiting this vulnerability requires an attacker to provide a malformed signed PKCS#7 to an application that verifies it. The impact of the exploit is just a Denial of Service, the PKCS7 API is legacy and applications should be using the CMS API instead. For these reasons the issue was assessed as Low severity. The FIPS modules in 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the PKCS#7 parsing implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4, 3.3, 3.0, 1.1.1 and 1.0.2 are vulnerable to this issue.

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
openssl.base	3.0.0.0	3.0.16.1000

Link

AIX/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 optimizer 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.

CWE: CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection')

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

- **VIOSUPGRADE DUPLICATES ENTRY IN CRON ROOT**
  After viosugprade, the cron root may duplicate an entry.
  EXAMPLE:
  ```
  # crontab -l | grep mail
  0 * * * * /usr/ios/cli/cron_mail_check.sh 2>/dev/null
  0 * * * * /usr/ios/cli/cron_mail_check.sh 2>/dev/null
  ```
  Link

- **BACKUPIOS FAILS WITH SAVEVG ERROR**
  backupios command fails to backup other VG data :
  For example:
  ```
  $ backupios -file /backup/mksysb.file -nomedialib 2>&1
  0512-009 savevg: Invalid or missing Volume Group Name.
  Usage:  savevg [-X] [-V] [-i] [-m] [-e] [-b blocks]\
   [-f device] [-p] [-v] [-r] [-a] [-A] [-Z] [-P]\
   [-x filename] [-T] vgName

  -X      Expand /tmp if needed.
  -V      Verify backup readability (tape only).
  ```
  Local fix
  Use the "-nosvg" option to not save other VG data.
  Link

PowerHA alerts:

- **High Impact / Highly Pervasive APAR IJ57286 IBM.SoftwareRM subsystem may kill all processes on PowerHA node**
  IBM.SoftwareRM subsystem may kill all processes on PowerHA node (AIX 7.3)
  Risk categories
  System Outage
  Due to a memory leak and incorrect initialisation, the RSCT subsystem IBM.SoftwareRM may kill some or all processes on a PowerHA node.
  Link

- **APAR IJ57270 Potential undetected data loss after PowerHA failover, during jfs2 filesystem recovery (PowerHA 7.2)**
  Potential undetected data loss after PowerHA failover, during jfs2 filesystem recovery
  Risk categories
  Data Loss
  When a PowerHA node acquires a jfs2 filesystem that had not been cleanly unmounted, such as after a crash or halt, the filesystem log may not be replayed when fsck is executed on the filesystem.
  This may result in undetected data loss as the filesystem is brought to a consistent state without replaying the log.
  Link

GPFS / Scale alerts:

- **Recovery group creation or disk replacement fails due to incorrect drive format in NVMe or IBM FlashCore Module**
  Recovery group (RG) creation or drive replacement might fail if an IBM FCM or industry-standard NVMe drive is formatted with a block size other than 4K+0B. An incorrect drive format might lead to I/O errors during these operations. In such cases, verify whether any existing or newly added drive is incorrectly formatted. Then, determine whether the drive is an IBM FCM or an industry-standard NVMe. And, if the drive with incorrect format is not currently in use by GNR, manually reformat it to 4K+0B.
  Users Affected
  This issue may affect clients that use IBM Storage Scale Systems (such as IBM Storage Scale System 3500 or IBM Storage Scale System 6000) that include IBM FCM or standard NVMe drives.
  Link

Keep safe and best wishes for the second quarter
Red, Belisama