Belisama

May Newsletter

Subscribe/Unsubscribe

Greetings all,
I trust that you are all keeping well?
We have been busy preparing for a couple of customers to migrate their workloads to newer hardware. In most instances this is a relatively painless tasks – only really an issue if care hasn't been taken to keep their environment up to date. This is when we see clear proof that having a consistent, well managed (automated!) Power environment more than pays back the effort in getting it to that point.

A few updates to share

- Submissions for TechXchange in Orlando have closed, now I am looking forward to seeing the Agenda, and of course, getting my sessions organised (hopefully!)

Quick bites

IBM i - maximising uptime
There was an interesting IBM community session last week "The Future of Enterprise Resilience for IBM i: Maximising Uptime in an Uncertain Business Environment", for details check the link.
Link

TCP tuning to improve WAN connections between two AIX LPARs
For details, see the link below, but in summary, the support article is suggesting:

- tcp_sendspace=1048576
- tcp_recvspace=1048576
- sb_max=2097152
- rfc1323=1
- tcp_nodelayack=0
- sack=1
- tcp_cubic=1
- mtu_bypass=on
- tcp_init_window=10
- hstcp=1

Link

IBM Power announcements
The May Power announcements:

- IBM and Red Hat offer new Standard support options for Red Hat AI Inference portfolio
- IBM Power Expert Care offers additional Committed Maintenance Service Levels
- IBM Concert Subscription for Power v2.4.0 Extend vulnerability management to IBM i

Introducing IBM Sovereign Core for Managed Services and IT Services Providers
Discover how IBM Sovereign Core enables Managed Service Providers and IT Service Providers to deliver secure, confirmed sovereign, and AI-ready environments. This session covered the digital sovereignty landscape, product capabilities, packaging, and roadmap, with a focus on supporting watsonx driven AI services.
Link

In case you missed ….

- **Rehost, Replatform, and Refactor at Your Own Pace: Modernising Virtualisation with IBM Fusion and Red Hat OpenShift**
  This session was presented by Mike Burkhart, Technical Product Manager, IBM Fusion, IBM
  Link
- **Power Systems VUG May 2026: IBM Power Cyber Vault for AIX**
  In today's threat landscape, cyber resilience is no longer optional, it's a critical requirement. This session explored the growing need to protect IBM Power environments from increasingly sophisticated threats such as ransomware and data corruption, and why traditional backup and recovery strategies are no longer sufficient.
  You'll also learn how the solution anticipates threats and minimises data loss through integrated capabilities including IBM PowerSC, FlashCore Module (FCM4), and IBM Zero Trust Execution for AIX.
  Link

Coming soon

- **Preparing IT Leaders for the Oracle 26ai Journey**
  This presentation for the Power Global group will be held on Tuesday 23/6/26 21:00 AEST/19:00 SGT
  Link

Redbooks and Redpapers

- **IBM Storage Scale: Working With Abstract Data**, Draft Redbook, 09 May 2026,
  Link

- **IBM Power Virtual Server with VPC Landing Zone**
  , Redpiece, 01 May 2026,
  Link

IBM alerts and notices

AIX alerts:

- **Resolving the EFS Issue for Non-Root: Problem initialising EFS framework**.
  Users are encountering an error when attempting to use the EFS (Encrypted File System) framework as a non-root user. The specific error message is
  Error: Problem initialising EFS framework. Please install latest version of clic.rte
  Cause
  Modification of Security Boot Configuration:
  The following line was removed or commented out in the /etc/inittab file:
  securityboot:2:bootwait:/etc/rc.security.boot>/dev/console 2>&1
  If the line is commented out but the system is not rebooted, the EFS framework works fine for non-root users. But if the line is commented out and the system is rebooted, non-root users encounter the EFS initialisation error for any EFS-related commands.
  Resolving The Problem
  To resolve the EFS initialisation issue for non-root users, follow these steps:
  - Restore the Security Boot Configuration line:
  - Uncomment/Add the below line in the /etc/inittab file
    securityboot:2:bootwait:/etc/rc.security.boot>/dev/console 2>&1
  - Reboot the System:

  Link

- **Multiple vulnerabilities impact AIX due to OpenSSL**
  Vulnerabilities in OpenSSL could send contents of an uninitialised memory buffer (CVE-2026-31790), cause a use-after-free (CVE-2026-28387), cause a NULL pointer dereference (CVE-2026-28388, CVE-2026-28389, CVE-2026-28390), or lead to a buffer overflow (CVE-2026-31789). OpenSSL is used by AIX as part of AIX's secure network communications.
  Vulnerability Details
  CVE-2026-31790 - Issue summary: Applications using RSASVE key encapsulation to establish a secret encryption key can send contents of an uninitialised memory buffer to a malicious peer. Impact summary: The uninitialised buffer might contain sensitive data from the previous execution of the application process which leads to sensitive data leakage to an attacker. RSA_public_encrypt() returns the number of bytes written on success and -1 on error. The affected code tests only whether the return value is non-zero. As a result, if RSA encryption fails, encapsulation can still return success to the caller, set the output lengths, and leave the caller to use the contents of the ciphertext buffer as if a valid KEM ciphertext had been produced. If

applications use EVP_PKEY_encapsulate() with RSA/RSASVE on an attacker-supplied invalid RSA public key without first validating that key, then this may cause stale or uninitialised contents of the caller-provided ciphertext buffer to be disclosed to the attacker in place of the KEM ciphertext. As a workaround calling EVP_PKEY_public_check() or EVP_PKEY_public_check_quick() before EVP_PKEY_encapsulate() will mitigate the issue. The FIPS modules in 3.6, 3.5, 3.4, 3.3, 3.1 and 3.0 are affected by this issue.
CVE-2026-28387- Issue summary: An uncommon configuration of clients performing DANE TLSA-based server authentication, when paired with uncommon server DANE TLSA records, may result in a use-after-free and/or double-free on the client side. Impact summary: A use after free can have a range of potential consequences such as the corruption of valid data, crashes or execution of arbitrary code. However, the issue only affects clients that make use of TLSA records with both the PKIX-TA(0/PKIX-EE(1) certificate usages and the DANE-TA(2) certificate usage. By far the most common deployment of DANE is in SMTP MTAs for which RFC7672 recommends that clients treat as 'unusable' any TLSA records that have the PKIX certificate usages. These SMTP (or other similar) clients are not vulnerable to this issue. Conversely, any clients that support only the PKIX usages, and ignore the DANE-TA(2) usage are also not vulnerable. The client would also need to be communicating with a server that publishes a TLSA RRset with both types of TLSA records. No FIPS modules are affected by this issue, the problem code is outside the FIPS module boundary.
CVE-2026-28388 - Issue summary: When a delta CRL that contains a Delta CRL Indicator extension is processed a NULL pointer dereference might happen if the required CRL Number extension is missing. Impact summary: A NULL pointer dereference can trigger a crash which leads to a Denial of Service for an application. When CRL processing and delta CRL processing is enabled during X.509 certificate verification, the delta CRL processing does not check whether the CRL Number extension is NULL before dereferencing it. When a malformed delta CRL file is being processed, this parameter can be NULL, causing a NULL pointer dereference. Exploiting this issue requires the X509_V_FLAG_USE_DELTAS flag to be enabled in the verification context, the certificate being verified to contain a freshestCRL extension or the base CRL to have the EXFLAG_FRESHEST flag set, and an attacker to provide a malformed CRL to an application that processes it. The vulnerability is limited to Denial of Service and cannot be escalated to achieve code execution or memory disclosure. 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 affected code is outside the OpenSSL FIPS module boundary.
CVE-2026-28389 - Issue summary: During processing of a crafted CMS EnvelopedData message with KeyAgreeRecipientInfo a NULL pointer

dereference can happen. Impact summary: Applications that process attacker-controlled CMS data may crash before authentication or cryptographic operations occur resulting in Denial of Service. When a CMS EnvelopedData message that uses KeyAgreeRecipientInfo is processed, the optional parameters field of KeyEncryptionAlgorithmIdentifier is examined without checking for its presence. This results in a NULL pointer dereference if the field is missing. Applications and services that call CMS_decrypt() on untrusted input (e.g., S/MIME processing or CMS-based protocols) are vulnerable. The FIPS modules in 3.6, 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the affected code is outside the CVE-2026-28390 - Issue summary: During processing of a crafted CMS EnvelopedData message with KeyTransportRecipientInfo a NULL pointer dereference can happen. Impact summary: Applications that process attacker-controlled CMS data may crash before authentication or cryptographic operations occur resulting in Denial of Service. When a CMS EnvelopedData message that uses KeyTransportRecipientInfo with RSA-OAEP encryption is processed, the optional parameters field of RSA-OAEP SourceFunc algorithm identifier is examined without checking for its presence. This results in a NULL pointer dereference if the field is missing. Applications and services that call CMS_decrypt() on untrusted input (e.g., S/MIME processing or CMS-based protocols) are vulnerable. The FIPS modules in 3.6, 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the affected code is outside the OpenSSL FIPS module boundary.

CVE-2026-31789 - Issue summary: Converting an excessively large OCTET STRING value to a hexadecimal string leads to a heap buffer overflow on 32 bit platforms. Impact summary: A heap buffer overflow may lead to a crash or possibly an attacker controlled code execution or other undefined behavior. If an attacker can supply a crafted X.509 certificate with an excessively large OCTET STRING value in extensions such as the Subject Key Identifier (SKID) or Authority Key Identifier (AKID) which are being converted to hex, the size of the buffer needed for the result is calculated as multiplication of the input length by 3. On 32 bit platforms, this multiplication may overflow resulting in the allocation of a smaller buffer and a heap buffer overflow. Applications and services that print or log contents of untrusted X.509 certificates are vulnerable to this issue. As the certificates would have to have sizes of over 1 Gigabyte, printing or logging such certificates is a fairly unlikely operation and only 32 bit platforms are affected, this issue was assigned 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 affected code is outside the OpenSSL FIPS module boundary.

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
openssl.base	3.0.0.0	3.0.16.1000

Link

Power9 Firmware:

- **HIPER Security issue: A security problem was fixed for CVE-2026-22796**
  The latest service pack 950.G1/950.H0 is now available for system firmware levels VL950, VM950, and VH950.
  Visit Fix Central for all the latest updates.
  Link

PowerVC alerts:

- **Erlang OTP inets httpd Vulnerable to HTTP Request Smuggling via Duplicate Content-Length Headers**
  Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in Erlang OTP (inets httpd module) allows HTTP Request Smuggling. This vulnerability is associated with program files lib/inets/src/http_server/httpd_request.erl and program routines httpd_request:parse_headers/7. The server does not reject or normalise duplicate Content-Length headers. The earliest Content-Length in the request is used for body parsing while common reverse proxies (nginx, Apache httpd, Envoy) honour the last Content-Length value. This violates RFC 9112 Section 6.3 and allows front-end/back-end desynchronisation, leaving attacker-controlled bytes queued as the start of the next request. This issue affects OTP from OTP 17.0 until OTP 28.4.1, OTP 27.3.4.9 and OTP 26.2.5.18, corresponding to inets from 5.10 until 9.6.1, 9.3.2.3 and 9.1.0.5.
  Vulnerability Details
    CVE-2026-23941 - Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in Erlang OTP (inets httpd module) allows HTTP Request Smuggling. This vulnerability is associated with program files lib/inets/src/http_server/httpd_request.erl and program routines httpd_request:parse_headers/7. The server does not reject or normalise duplicate Content-Length headers. The earliest Content-Length in the request is used for body parsing while common reverse proxies (nginx, Apache httpd, Envoy) honor the last Content-Length value. This violates RFC 9112 Section 6.3 and allows front-end/back-end desynchronisation, leaving attacker-controlled bytes queued as the start of the next request. This issue affects OTP from OTP 17.0 until OTP 28.4.1, OTP 27.3.4.9 and OTP 26.2.5.18, corresponding to inets from 5.10 until 9.6.1, 9.3.2.3 and 9.1.0.5.

CVE-2026-23942 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Erlang OTP (ssh_sftpd module) allows Path Traversal. This vulnerability is associated with program files lib/ssh/src/ssh_sftpd.erl and program routines ssh_sftpd:is_within_root/2. The SFTP server uses string prefix matching via lists:prefix/2 rather than proper path component validation when checking if a path is within the configured root directory. This allows authenticated users to access sibling directories that share a common name prefix with the configured root directory. For example, if root is set to /home/user1, paths like /home/user10 or /home/user1_backup would incorrectly be considered within the root. This issue affects OTP from OTP 17.0 until OTP 28.4.1, OTP 27.3.4.9 and OTP 26.2.5.18, corresponding to ssh from 3.0.1 until 5.5.1, 5.2.11.6 and 5.1.4.14.

Affected Products and Versions

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

Link

- **Relative Path Traversal, Improper Isolation or Compartmentalisation vulnerability in erlang otp**

  Relative Path Traversal, Improper Isolation or Compartmentalisation vulnerability in erlang otp erlang/otp (tftp_file modules), erlang otp inets (tftp_file modules), erlang otp tftp (tftp_file modules) allows Relative Path Traversal. This vulnerability is associated with program files lib/tftp/src/tftp_file.erl, src/tftp_file.erl. This issue affects otp: from 17.0, from 07b8f441ca711f9812fad9e9115bab3c3aa92f79; otp: from 5.10 before 7.0; otp: from 1.0.

  Vulnerability Details

  CVE-2026-21620 - Relative Path Traversal, Improper Isolation or Compartmentalisation vulnerability in erlang otp erlang/otp (tftp_file modules), erlang otp inets (tftp_file modules), erlang otp tftp (tftp_file modules) allows Relative Path Traversal. This vulnerability is associated with program files lib/tftp/src/tftp_file.erl, src/tftp_file.erl. This issue affects otp: from 17.0, from 07b8f441ca711f9812fad9e9115bab3c3aa92f79; otp: from 5.10 before 7.0; otp: from 1.0.

  Affected Products and Versions

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

  Link

- **Update on PowerVC fixes**

The following is a list of recent notices/fixes for PowerVC:

- libsodium vulnerability: invalid elliptic curve point validation in crypto_core_ed25519_is_valid_pointhttps://www.ibm.com/support/pages/node/7271554?myns=swgother&mynp=OCSS2MT9&mync=E&cm_sp=swgother-_-OCSS2MT9-_-E

- Requests SSL Verification Issue Fixed in 2.32.0
- Werkzeug safe_join function allows path segments with Windows device names containing file extensions or trailing spaces
- Flask Vary Cookie Header Vulnerability: Use of Cache Containing Sensitive Information Fixed in 3.1.3
- Werkzeug Safe Join Function Vulnerability: Path Segments with Windows Device Names Prior to Version 3.1.4
- ACE Vulnerability in QOS.CH Logback-core 1.5.24: Class Instantiation via Compromised Configuration File
- Safe Join Function Vulnerability Fixed in Werkzeug v3.1.6
- Lodash Prototype Pollution Vulnerability in Versions 4.0.0-4.17.22
- Netty CRLF Injection in HttpRequestEncoder: Request Smuggling Vulnerability Fixed in 4.1.129.Final and 4.2.8.Final
- Axios HTTP/2 Session Cleanup Logic State Corruption Bug Fixed in 1.13.2
- Denial of Service in urllib3 via Unbounded Decompression of Redirect Responses
- Jetty URI Parser Differences and Potential Security Implications
- urllib3 Unbounded Decompression Chain Enables Denial of Service
- qs Array Limit Bypass via Comma Parsing Enables Denial of Service
- pyasn1 Uncontrolled Recursion in ASN.1 Decoding Enables Denial of Service
- UltraJSON Memory Leak in Large Integer Parsing Enables Denial of Service
- pyasn1 Memory Exhaustion via Malformed RELATIVE-OID Leads to Denial of Service
- jsPDF addImage Method Vulnerable to DoS via Malicious Image Dimensions
- PyJWT Fails to Validate Critical (crit) Header Parameter, Allowing Token Acceptance
- pyOpenSSL TLS SNI Callback Exception Handling Flaw Allows Security Bypass
- Cryptography Missing Subgroup Validation in EC Public Keys Enables ECDH Key Leakage and ECDSA Forgery
- Denial of Service in Axios via Malicious __proto__ in Configuration Object
- Jackson-core Async JSON Parser Bypasses maxNumberLength Constraint Leading to DoS
- Lodash Prototype Pollution Bypass in _.unset and _.omit via Array Path Segments
- Axios NO_PROXY Bypass via Improper Hostname Normalisation Leads to SSRF

GPFS/Scale alerts:

- **Vulnerability in Linux kernel crypto subsystem could allow local privilege escalation (CVE-2026-31431)**
  IBM Storage Scale Systems is affected by a security vulnerability identified in the Linux kernel's cryptographic interface (CVE-2026-31431) that could allow a local user with low privileges to escalate to root privileges. The vulnerability has a CVSS score of 7.8 (High) and requires local system access to exploit on RHEL 8 and 9.
  Vulnerability Details
  CVE-2026-31431 - In the Linux kernel, the following vulnerability has been resolved: crypto: algif_aead - Revert to operating out-of-place This mostly reverts commit 72548b093ee3 except for the copying of the associated data. There is no

benefit in operating in-place in algif_aead since the source and destination come from different mappings. Get rid of all the complexity added for in-place operation and just copy the AD directly.

Affected Products and Versions

Affected Product(s)	Version(s) (RHEL8 and RHEL9 platforms only)
IBM Storage Scale System	6.1.0.0 - 6.1.9.8
IBM Storage Scale System	6.2.0.0 - 6.2.3.5
IBM Storage Scale System	7.0.0.0 - 7.0.0.2

Link

Keep safe and hope to see you in Orlando.

Red, Belisama