Belisama

October Newsletter

Subscribe/Unsubscribe

Greetings all,
I hope that all those in Atlanta (got it right this time!) are funding enough sessions on Power/AIX/i etc to satisfy the craving (and keep the Power spirit alive!). Anyway I trust that the networking keep the enthusiasm going.

A few updates to share

- New capabilities and enhancements with IBM i 7.6 refresh 3 and 7.5 refresh 9
  7.6
  7.5
- There are also some changes in subscriptions for i (migrate while active) and some additional software inclusion and education. See the Power announcements,
  Link
- Number of big changes announced for AIX, PowerVC, PowerSC, PowerVM and PowerHA (see below).
- Have been working with a couple of clients, looking at ways to reduce network latency while still keeping the advantages of virtualisation. SR-IOV (able to split network adapter and share amongst guest – but no LPM); vNIC (allows LPM) and HNV. Hybrid Network Virtualisation, which combines the best of both, is looking like the way to go. I found this link as a good starting point: link.
- Resource Groups introduced in Power11. Resource Groups allow the administrator to create a "group" of processor cores. This allows the hypervisor to control which physical cores can be allocated to individual LPARs. This allows greater control over Processor affinity, as well as memory affinity with appropriate planning.
- Planning your Power maintenance?
  Check the P9, P10 and P11 System firmware planning schedule – updated for 2026 / 2027.
  Start planning now for next year.
  Link

Quick bites

IBM AIX and Availability Enhancements, planned availability date: 4/12/26
Changes announced:

- AIX Standard Edition 7.3 TL5
- AIX 7 Enterprise Edition 1.16
- PowerHA SystemMirror Standard and Enterprise Edition 7.2.11
- PowerSC 2.4

IBM Champion
2022
IBM

AIX 7.3 TL5

- AIX UDP networking has been enhanced to support improved performance and scalability on multi-core LPARs, including packet processing across multiple network interfaces.
- AIX Virtual Ethernet includes multi-buffer posting enhancements on systems running Power System firmware 1120 or later to reduce bottlenecks and improve throughput.
- The maximum supported memory configuration for AIX is increased to 64 TB.
- JFS2 Concurrent I/O has been enhanced for synchronous and asynchronous I/O operations involving Allocated but not recorded (ABNR) extents and file holes.
- Dynamic Resource Manager (DRMGR) has been enhanced to improve the performance of CPU add and remove operations.

Maximise availability and reliability

Live Kernel Update (LKU) enhancements have been introduced in the following areas:

- LKU check-pointing: Updates to check-pointing for systems with large shared memory, heap, stack, and mmap configurations.
- File descriptor check pointing: Updates support check-pointing of non-shared file descriptors.
- LPAR resource configuration: Support for resizing LPAR maximum CPU and memory resources during LKU using PowerVC compute templates.
- Processor Compatibility Mode: Support for changing processor compatibility mode during LKU through HMC and PowerVC.
- Reduced LKU restrictions:
    - LPARs with PCI-DSS or CIS PowerSC security profiles applied can now be used with LKU.
    - The previous restriction associated with configurations supporting more than 64K file descriptors has been removed.
    - LKU boot processing: LKU now uses a single surrogate boot.
- AHAFS has been enhanced to support filesystem level monitoring of file operation events.
- AIX networking and tcpdump have been enhanced to support capture of RoCE packets.
- Geographic Logical Volume Manager (GLVM) introduces a tuneable for application I/O resumption following varyonvg.
- AIX `raso` command (for RAS tuning) introduces the `dump_on_reboot` tuneable. When set to 1, the tuneable causes a system dump to be initiated during a graceful system reboot.

Protect data from core to cloud

- AIX IPsec filter is optimised for better performance in high network throughput scenarios.
- OpenSSL 3.5 is included with this release of AIX. OpenSSL 3.5 includes support for post-quantum cryptographic algorithms.
- OpenSSH 10.5 is included with this release of AIX. The release includes support for post-quantum cryptographic algorithms.

IBM Champion
2022
IBM

- sudo is included with the AIX operating system to provide privilege management capabilities.
- AIX Trusted Execution supports a permissive mode in which policy violations are logged without enforcement of the corresponding policy.
- AIX cryptographic discovery introduces a framework for identifying and assessing cryptographic usage within the environment.
- Network Installation Manager (NIM) supports a CA-signed certificate mode for secure communication between the NIM master and NIM clients using certificates issued by a trusted Certificate Authority (CA).

Streamline insights and automation for enhanced administration efficiency

The AIX Collection for Ansible introduces several significant enhancements in 2026, expanding automation, event-driven management, and system administration capabilities for AIX environments.

The following Event-Driven Ansible (EDA) plugins have been added to enable automated responses to system and infrastructure events:

- flrt_monitor
- aix_filesystem_watch
- aix_file_watch
- errpt_monitor
- audit_monitor
- disk_watch

The AIX Ansible collection now includes several new modules to simplify network and system administration tasks:

- errclear
- traceroute
- genfilt
- tcpdump
- nslookup
- ssh_config

New roles have been introduced to streamline common administration and security tasks:

- ipsec
  A role for configuring and managing IPsec tunnels.
- Populate lvupdate.data
  Automates the creation and maintenance of the lvupdate.data file.
- IPsec XML Management
  Automates the management of XML configuration files used by IPsec.

New demonstration playbooks have been added to showcase the capabilities and usage of the newly introduced roles, modules, and EDA plugins, helping users accelerate adoption and deployment.

The AIX Collection for Ansible is available through Ansible Galaxy for IBM AIX users. Community feedback and contributions are encouraged. For customers using the Red Hat Ansible Automation Platform, the same content is also available through Ansible Automation Hub as fully supported content.

IBM Champion
2022
IBM

Additional enhancements
The following Open Source based programs included with AIX have been updated to newer versions as follows:

- OpenSSL 3.5.8
- OpenSSH 10.5
- ksh93 u+m/1.0.10
- Python 3.14.7
- Perl 5.42.0
- BIND 9.18.49
- rsyslog 8.2412.0

And:

- The `ping` command has been enhanced to optionally send and receive UDP or TCP probes, providing an alternative when ICMP traffic is blocked by network policies. This enables latency measurement between LPARs using UDP or TCP protocols. The utility can also operate as an echo server, returning received packets unchanged to ensure compatibility with standard echo clients. In addition, all existing ICMP ping options are supported for UDP and TCP probe operations where applicable. These enhancements are supported only for IPv4 networks.
- The Simple Authentication and Security Layer (SASL) library has been enhanced to provide support for OpenSSL 3.0. This update ensures compatibility with OpenSSL 3.0-based environments, enabling applications that rely on SASL for authentication and security services to take advantage of the latest cryptographic framework and security enhancements.
- ksh93 has been upgraded from ksh93u+ to ksh93 u+m/1.0.10, incorporating community bug fixes, security updates and POSIX compliance enhancements.
- The LLDB (LLVM community's Low Level Debugger) has been enhanced with support for disassembly-related debugging, watchpoints, 32-bit live debugging, multithreaded application debugging, improved STL compatibility, and numerous stability and quality improvements. LLDB for AIX is available as a web download package from AIX web download site.

Recent AIX Toolbox for Open Source Software updates

- Several important new packages have been added to the AIX Toolbox, including postgresql18-vector, lmdb, opentelemetry-cpp, otelcol, uv, ripgrep, cfengine, python3-pydantic-core, and z3.
- In addition, many existing packages have been updated to their latest community-supported versions, and security fixes have been delivered for numerous packages to help maintain a secure and up-to-date software environment.
- The introduction of new packages, updates to existing packages, and notifications of security updates are announced in the AIX Open Source discussion forum. There, users can also interact with the IBM open source team and other users and post questions about packages.

See link

IBM Champion
2022
IBM

IBM AIX 7 Enterprise Edition 1.16

IBM has updated the AIX 7 Enterprise Edition and its corresponding subscription offering to version 1.16 The bundled software components offered with AIX 7 Enterprise Edition 1.16 (5765-CD3 and 5765-2E1) now includes:

- IBM AIX 7.3 TL5 or IBM AIX 7.2 TL5
- IBM PowerVC for Private Cloud V3
- IBM PowerSC 2.4
- IBM VM Recovery Manager DR 1.10
- IBM Tivoli Monitoring 6.3

The bundle components are updated as follows:

- AIX 7.3 TL4 has been updated to TL5
- IBM PowerVC for Private Cloud has been updated from 2.3.3 to new version IBM PowerVC for Private Cloud V3

Additional information:

- Clients with active Software Maintenance (SWMA) or subscriptions for earlier versions of AIX Standard Edition or AIX Enterprise Edition are entitled to upgrade at no charge. To update, download, or install, see the IBM Entitled Systems Support website.
- Clients can choose either AIX 7.3 TL5 or AIX 7.2 TL5.
- Clients selecting AIX 7.2 TL5 can later upgrade to AIX 7.3 TL5 at any time, provided SWMA or subscription is current.

Link

PowerSC 2.4

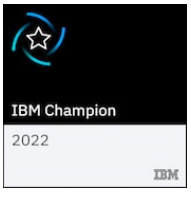
CVE/CVSS visibility for AIX fixes (Compliance Automation)
PowerSC Compliance Automation displays Common Vulnerabilities and Exposures (CVE) identifiers and Common Vulnerability Scoring System (CVSS) scores associated with proposed AIX fixes in the PowerSC graphical user interface (GUI).
The information provides administrators with vulnerability identifiers and severity information associated with applicable AIX fixes for use in remediation assessment and prioritisation activities.
Virtual Trusted Platform Module (vTPM) 2.0 support

- PowerSC 2.4 introduces initial support for vTPM 2.0. The PowerSC GUI displays vTPM-related information for manually configured partitions.

Centre for Internet Security (CIS) Ubuntu profile

- PowerSC Compliance Automation adds a compliance profile based on the CIS Benchmark for Ubuntu for supported Power and x86 endpoints. The profile enables administrators to assess Ubuntu system configurations against the applicable CIS Benchmark recommendations and, where supported, apply remediation through the PowerSC Compliance Automation workflow.

Link



PowerHA SystemMirror for AIX

IBM PowerHA SystemMirror 7.2.11 introduces the following enhancements:

Policy Based High Availability (PBHA) and Policy Based Replication (PBR)

Unified application-aware HA and DR orchestration across clustering and replication with automated failover and recovery for improved continuity, lower RTO, reduced operational complexity for business critical workloads.

Policy Based Replication (PBR) with Partition Support (PowerHA and VMRM)

Enhanced partition-aware replication for PBR

PowerHA 7.2.11 release extends PBR capabilities with support for partition-aware storage replication, enabling organisations to protect and recover data at a more granular level within replicated storage environments, with following benefits :

- Partition level protection and recovery using storage replication technologies.
- Enables partition-aware protection compared to system replication models by leveraging underlying synchronous and asynchronous storage replication across supported IBM storage platforms.
- Accelerates recovery of business critical applications while reducing downtime and avoiding failover of unaffected workloads.
- Reduced operational complexity through integration with existing PBR workflows.
- Enhanced disaster recovery efficiency while maintaining consistent storage based data protection.

PowerVS Overlay Network Support (PowerHA)

Simplified cloud networking maintains connectivity during resource group failover operations and supports workload mobility across cloud environments.

- Maintains application accessibility during failover without requiring manual network configuration changes, preserving connectivity for users, client applications, and dependent business services.
- Automatically preserves network communication paths as workloads move between sites or cloud environments, reducing service disruption and downtime.
- Supports workload mobility across cloud environments so that critical applications remain available and accessible during planned migrations and unplanned failover events.

Sync and Async GLVM Assistant (PowerHA)

Guided deployment and validation for faster replication setup and DR readiness for faster setup with automation validation to accelerate adoption and improve DR readiness.

NFS Tie breaker priority support (PowerHA)

Consistent priority based arbitration for improved cluster stability and resiliency through improved cluster stability, recovery predictability, deployment flexibility across diverse environments, and prevent shared storage access conflict.

Resource group support (VMRM)

Enables PowerHA protection and management for additional resource group configurations, improving workload availability and operational flexibility.

Preemption of low priority VMs (VMRM)

IBM Champion
2022
IBM

Automatically prioritises critical workloads by reclaiming resources from lower priority virtual machines during capacity constraints.

Link

IBM Power Virtualisation and Platform Enhancements, planned availability date: 4/12/26

IBM offers the following IBM Power Virtualisation and Platform Enhancements:

- PowerVC for Private Cloud 3.0
  PowerVC delivers new capabilities simplifying virtualisation management, strengthening resiliency, and accelerating automation across IBM Power environments.
  - PowerVC software appliance supports x86 platforms (KVM image) for greater deployment flexibility.
  - Image node as a software appliance to accelerate installation and time-to-value.
  - Support for changing Virtual IP address (VIP) and node IP addresses to simplify network and infrastructure management.
  - Dynamic configuration updates that increase agility while reducing operational disruption, includes settings for processor capped or uncapped and Simplified Remote Restart
  - Enhanced notifications and alerting for improved visibility and faster issue resolution.
  - Configuration management tools that simplify PowerVC deployment and ongoing administration.
  - New Ansible modules for PowerVC to enable infrastructure-as-code and enterprise-scale automation.
- IBM PowerVM Novalink 3.0
  Updates in RSCT packages and now deployable as an appliance.
- IBM Virtual I/O Server (VIOS) 4.1.3
  VIOS 4.1.3 introduces new capabilities designed to improve performance, availability, and operational flexibility.
  - Enhanced Shared Ethernet Adapter (SEA) networking enables virtual Ethernet adapters and VLANs to be added dynamically to a SEA, reducing operational disruption and increasing network agility.
  - Multi-queue Virtual Ethernet Trunk Adapter increases packet-processing parallelism and enhances network performance.
  - Virtual Fibre Channel (NPIV) Quality of Service (QoS) enables administrators to better align virtualised storage performance with application Service Level Agreements (SLAs), delivering more consistent and predictable workload outcomes.
  - Higher NPIV IOPS for small-block workloads, delivering improved storage performance and greater efficiency.

IBM Champion
2022
IBM

    - Balanced LPAR placement for NPIV adapters during LPM operations optimises virtual adapter distribution across FC HBA resources, improving scalability, resiliency, and overall infrastructure utilisation.
    - Improved Live Partition Mobility (LPM) validation strengthens pre-migration network verification between Mobility Service Partitions (MSPs), helping improve migration reliability and reduce the risk of unexpected issues.
- IBM Power HMC 11.2.1121 and vHMC 11.2.1121
    - IBM Power Hardware Management Console (HMC) 11.2.1121 and IBM Power Virtual Hardware Management Console (vHMC) 11.2.1121 deliver enhancements that improve availability, workload mobility, and operational simplicity for IBM Power environments.
    - Non-disruptive network updates enable dynamic addition of vENT and VLANs to Shared Ethernet Adapters (SEA) without impacting running workloads.
    - Migratable SR-IOV RoCE logical ports support IBM Db2 Mirror for i environments, enabling workload mobility and increasing flexibility for high-availability deployments.
    - Fibre Channel port validation bypass during Live Partition Mobility (LPM) provides added flexibility and storage support.

Link

Software withdrawal from marketing and support discontinuance

- IBM AIX 7 Enterprise Edition
- IBM AIX 7 Enterprise Edition subscription
- IBM PowerSC
- IBM PowerSC Subscription
- PowerVC for Private Cloud V2
- IBM PowerVC Private Cloud subscription

Details

Program #	Program name	Version	EoS	Effective date	Replacement
5765-CD3	AIX 7 Enterprise Edn	1.15	30/4/28	4/12/26	1.16
5765-2E1	AIX 7 Ent Edn Subs	1.15	30/4/28	4/12/26	1.16
5765-SC2	PowerSC	2.3	30/4/28	4/12/26	2.4
5765-S2S	PowerSC Subs	2.3	30/4/28	4/12/26	2.4
5765-VC	PowerVC for Priv Cloud	V2	30/4/28	4/12/26	V3
5765-Z14	PowerVC Priv Cld Subs	Subs	30/4/28	4/12/26	V3

Link

New 32GB and 64GB 2U DDIMM support on Power servers E1180 and E1150

To provide customers with greater flexibility amid global memory supply chain challenges, IBM is introducing new 2U Differential Dual In-line Memory Module (DDIMM) options featuring DDR5 technology for IBM Power11 scale-up systems.

The new 2U DDIMM offerings provide a more cost-effective memory alternative to existing 4U DDIMM options. While they offer a lower level of redundancy, they maintain the performance and enterprise-class RAS capabilities required for business-critical workloads.

IBM Champion
2022
IBM

These new memory options help reduce overall system costs while enabling customers to scale applications efficiently without compromising functionality.
For IBM Power E1180

- 128 GB (4x32GB) DDR5 Memory 2U DDIMM
- 256 GB (4x64GB) DDR5 Memory 2U DDIMM

For IBM Power E1150

- 64GB (2 x 32GB) DDIMM (2U) 4000MHZ 16GBIT DDR5
- 128GB (2x64GB) DDIMM (2U), 4000MHZ 16GBIT DDR5

Link

Effective withdrawal date has been changed for selected Power features
The withdrawal date has changed from 27 February 2027 to 13 October 2026 for:

PCIe4 32Gb 4-port Optical Fibre Channel Adapter	EN2L
PCIe4 LPX 32Gb 4-port Optical Fibre Channel Adapter	EN2M
PCIe4 64Gb 2-port Optical Fibre Channel Adapter	EN2N

Link

Coming soon

- **Bob TV Episode 3**
  Join host Max Jesch, who welcomes Rynne Whitnah, Technical Lead AI Ecosystem at IBM, to explore ways to get more from IBM Bob while keeping token costs in check.
  Link

Redbooks and Redpapers

- **The Definitive Guide to IBM Storage FlashSystem and AIX Integration**, Draft Redbook, 15 October 2026
  Link

IBM alerts and notices

AIX/PowerVM alerts:

- **UPDATED bulletin for OpenSSL vulnerabilities impacting AIX**
  Vulnerabilities in OpenSSL: (CVE-2026-35189 - Memory exhaustion DoS), (CVE-2026-54872 - ECDSA/SM2 timing side-channel), (CVE-2026-77696 - SM2 timing side-channel),(CVE-2026-84782 - Out-of-Bounds Read), (CVE-2026-75805 - NULL pointer dereference DoS), (CVE-2026-75806 - DTLS connection termination DoS). OpenSSL is used by AIX as part of AIX's secure network communications.
  Details
  CVE-2026-75805 - Issue summary: A CMP client that requests certificate revocation on the basis of a PKCS#10 CSR may dereference a NULL pointer and terminate abnormally when processing a crafted revocation response. Impact

IBM Champion
2022
IBM

summary: The NULL pointer dereference happens on a read which leads to a crash and a Denial of Service for the affected client application. CWE: CWE-476: NULL-pointer dereference Description: A CMP client revoking a certificate has to tell the server which certificate to revoke, and may do so by supplying a PKCS#10 CSR instead of the certificate itself or its issuer name and serial number. This is 'openssl cmp -cmd rr -csr file' on the command line, or OSSL_CMP_exec_RR_ses() with the certificate supplied via OSSL_CMP_CTX_set1_p10CSR() through the API. A CSR does not contain the issuer name and serial number of the certificate, so the client does not send them. A server may optionally name the certificate it revoked in its response, and the client then compares that name against what it sent. Having sent neither an issuer name nor a serial number, it has nothing to compare against, and a server returning a specially crafted name causes the client to read from a NULL pointer and crash. The revocation response is checked for valid message protection before the affected code is reached, so an attacker must be a malicious or compromised CMP server, or a man-in-the-middle in possession of the secret used for message protection. Clients that identify the certificate to be revoked by a certificate or by issuer and serial number rather than by a PKCS#10 CSR are not affected. FIPS impact: no No FIPS modules are affected by this issue, as the CMP protocol implementation is outside the OpenSSL FIPS module boundary.

CVE-2026-75806 - Issue summary: An established DTLS 1.2 association using an AEAD cipher suite can be terminated by a single unauthenticated datagram whose encrypted fragment is shorter than the mandatory explicit IV and authentication tag overhead. Impact summary: An attacker who can send a datagram that is routed to an existing DTLS 1.2 association can tear that association down without knowing any key material. This is a Denial of Service limited to the targeted association. There is no memory safety or confidentiality impact. CWE: CWE-1284: Improper Validation of Specified Quantity in Input Description: In TLS 1.2 and DTLS 1.2 every record protected by an AEAD cipher suite carries an explicit IV followed by the ciphertext and an authentication tag. When decrypting such a record the record layer passed the record length to the cipher implementation before checking that the record was long enough to contain the explicit IV and the tag. For a record shorter than that overhead the cipher implementation rejected the impossible length, and the record layer treated this as an internal failure and raised a fatal internal_error alert instead of treating the record as one that failed authentication. In TLS 1.2 the same record causes a fatal internal_error alert instead of the expected bad_record_mac alert. Since any undecryptable record already terminates a TLS connection, this is a protocol conformance issue rather than a security issue in TLS. The fix validates the record length against the explicit IV and tag length before any AEAD processing, so that TLS reports bad_record_mac and DTLS silently discards

IBM Champion
2022
IBM

the record. FIPS impact: no The affected code is outside the FIPS module boundary.

CVE-2026-35189 - Issue summary: A certificate with many nameRelativeToCRLIssuer CRL distribution points causes disproportionate heap growth when OpenSSL caches X.509 extensions. Impact summary: Receiving a crafted certificate from a malicious peer can lead to significant memory pressure and possible Denial of Service in clients or in servers that solicit client certificates. CWE: CWE-770: Allocation of Resources Without Limits or Throttling Description: A certificate or a set of certificates that fits under the limit for size of certificates accepted from the peer (~100 KiB) can result in allocation of several hundred MiB of resident memory on the receiving side during a normal TLS handshake. This may be enough to crash the client or server, if multiple concurrent connections lead to similarly large memory allocations. The fix postpones processing of the CRL distribution points extensions in certificates to the time when the processed value is required for CRL processing. This avoids keeping large memory allocations for a long time when such certificates are received. FIPS impact: no The affected code is outside the FIPS module boundary.

CVE-2026-54872 - Issue summary: The generic elliptic-curve scalar multiplication used for ECDSA and SM2 signature operations with curves that do not have a dedicated implementation leaks information about the secret nonce through timing. Impact summary: An attacker able to measure signing times may learn information about the per-signature secret nonce, which over many signatures can, via a lattice / Hidden Number Problem attack, lead to recovery of the private key. CWE: CWE-208: Observable Timing Discrepancy Description: The generic elliptic-curve scalar multiplication used for curves that do not have a dedicated constant-time implementation pads the secret scalar with non-constant-time BIGNUM operations, so the time taken depends on the value of the secret scalar derived from the ECDSA and SM2 nonce. The leak is very small; observing it requires a large number of measurements. The effect is largest for curves whose group order lies on a machine-word boundary, such as brainpoolP384r1. Applications using ECDSA signing over the Brainpool and other generic prime curves, and SM2 signing on platforms that use the generic implementation, are vulnerable to this issue. The NIST curves P-256, P-384 and P-521 use dedicated constant-time implementations and are not affected. FIPS Impact: no The FIPS modules are not affected: the approved NIST curves used in the FIPS provider have dedicated constant-time implementations and do not use the affected code path.

CVE-2026-77696 - Issue summary: SM2 signature generation uses non-constant-time arithmetic on secret values, forming a timing side-channel. Impact summary: An attacker able to measure SM2 signing times may learn information about the per-signature secret nonce, which over many signatures can, via a lattice / Hidden Number Problem attack, lead to recovery of the

IBM Champion
2022
IBM

private key. CWE: CWE-208: Observable Timing Discrepancy Description: SM2 signature generation computes the signature value using variable-time BIGNUM operations on the secret nonce and the private key, so the time taken to produce an SM2 signature depends on these secret values, forming a timing side-channel. Applications performing SM2 signature generation are affected on all platforms. FIPS Impact: no SM2 is not a FIPS algorithm.

CVE-2026-84782 - Issue summary: The DTLS retransmission logic does not correctly handle a handshake message write that is suspended part-way through. The retransmitted message can be read past the message buffer and the retransmission overwrites the internal state the suspended write needs to resume correctly. Impact summary: The retransmitted message can disclose a heap memory to the peer as plaintext handshake data or cause a crash and a Denial of Service when the read reaches an unmapped memory region. CWE: CWE-125: Out-of-bounds Read Description: DTLS handshake messages can be written out in multiple fragments, and a write can suspend mid-message (returning WANT_WRITE) if the underlying transport temporarily cannot accept more data. While such a write is suspended, the DTLS retransmission timer may independently fire and ask the retransmission logic to resend an earlier, already-acknowledged-as-sent message from its retransmit queue. The retransmission logic reused the same internal buffer and position tracking as the message that was still being written, without resetting the position back to the start of the message being retransmitted. As a result the retransmission was read starting from wherever the suspended write had left off, producing a mislabelled message whose body was leftover bytes from the other, larger message still in flight - content that was never meant to be sent at that point, and which could run past the end of the allocated buffer. Separately, even when the retransmission is positioned correctly, allowing it to run to completion while another write is suspended overwrites the same shared bookkeeping that the suspended write depends on to resume. When the application later resumes the suspended write (via a subsequent SSL_read(), SSL_write(), SSL_accept(), or SSL_connect() call), it finds that bookkeeping in a state inconsistent with the message and aborts the process in a debugging build. The fix resets the retransmission's read position to the start of the message before resending, and skips retransmission entirely whenever a handshake write is still suspended, deferring to the next call that resumes it instead. FIPS impact: no The affected code is outside the FIPS module boundary.

Affected Products and Versions

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

IBM Champion
2022
IBM

The vulnerabilities in the following filesets are being addressed:

key_fileset = osrcaix

Fileset	Lower Level	Upper Level	KEY
openssl.base	3.0.0.0	3.0.21.1000	key_w_fs

Link

- **Security Bulletin: AIX is vulnerable to a denial of service due to NTP and tmux.** Multiple vulnerabilities in NTP and tmux could allow a remote attacker to cause Integer Overflow (CVE-2026-63384), Out-of-bounds Read (CVE-2026-63383), Memory Corruption (CVE-2026-63381, CVE-2026-63387, CVE-2026-63388), HTTP Request Smuggling / Header Injection (CVE-2026-63379, CVE-2026-63382, CVE-2026-63385).

  CVE-2026-63379 - Libevent is an event notification library. Prior to 2.1.13 and 2.2.2-alpha, libevent processes chunked HTTP trailers in http.c through evhttp_read_trailer and merges them into request headers. The fix introduces evhttp_parse_headers_impl_ and a temporary trailer header list. An unauthenticated remote attacker can place security-sensitive fields in trailers so that an upstream proxy and the libevent application interpret different effective headers, enabling header smuggling, authorization bypass, proxy-header spoofing, or cache poisoning. The fix parses trailers into a temporary header list and discards them instead of merging them into req-input_headers. This issue is fixed in versions 2.1.13 and 2.2.2-alpha.

  CVE-2026-63381 - Libevent is an event notification library. Prior to 2.1.13 and 2.2.2-alpha, libevent has a use-after-free in buffer.c when evbuffer_add_buffer_reference processes an output buffer whose out_total_len is zero. evbuffer_free_all_chains frees the initial empty chain without resetting outbuf-first, outbuf-last, or outbuf-last_with_datap, and APPEND_CHAIN_MULTICAST subsequently dereferences the dangling chain pointer. A caller that can drive this buffer state can cause memory corruption or a process crash. This issue is fixed in versions 2.1.13 and 2.2.2-alpha.

  CVE-2026-63382 - Libevent is an event notification library. Prior to 2.1.13 and 2.2.2-alpha, the libevent evhttp parser in http.c inconsistently handles duplicate Transfer-Encoding headers, comma-separated Transfer-Encoding values, and bare line feeds in chunked framing. evhttp_find_header can select only the first header, evhttp_check_transfer_encoding_ was absent so the previous whole-string comparison fails to recognize valid lists ending in chunked, and evhttp_handle_chunked_read uses EVBUFFER_EOL_CRLF rather than EVBUFFER_EOL_CRLF_STRICT, accepting bare LF chunk terminators. When libevent is deployed behind a proxy that frames the same request differently, an unauthenticated remote attacker can desynchronize request boundaries and smuggle a second request, potentially bypassing access controls or poisoning caches. This issue is fixed in versions 2.1.13 and 2.2.2-alpha.

IBM Champion
2022
IBM

CVE-2026-63383 - Libevent is an event notification library. Prior to 2.1.13 and 2.2.2-alpha, libevent can read beyond a contiguous evbuffer region in event_tagging.c when decode_tag_internal requests at most five bytes from evbuffer_pullup but iterates using the full logical buffer length. A fragmented evbuffer containing a six-byte malformed tag can therefore advance past the pullup window and trigger an out-of-bounds read, which can crash a process that decodes attacker-controlled tagged RPC data. This issue is fixed in versions 2.1.13 and 2.2.2-alpha.

CVE-2026-63384 - Libevent is an event notification library. Prior to 2.1.13 and 2.2.2-alpha, libevent has an incorrect integer conversion in event_tagging.c when evtag_unmarshal_header uses evtag_decode_int to decode an attacker-controlled uint32 payload length and returns it as a signed int. Values above INT_MAX become negative or truncated, and evtag_unmarshal_string can use the converted value in allocation sizing, producing a wrapped large allocation request and denial of service. This issue is fixed in versions 2.1.13 and 2.2.2-alpha.

CVE-2026-63385 - Libevent is an event notification library. Prior to 2.1.13 and 2.2.2-alpha, libevent has two HTTP parsing weaknesses in http.c. evhttp_decode_uri_internal decodes percent-encoded %00 bytes into literal NUL characters, which can cause downstream C string operations to truncate a path and bypass validation performed on a different representation. evhttp_header_is_valid_value also accepts obsolete line folding in header values containing carriage return or line feed characters, allowing a proxy and libevent to interpret headers differently and enabling header injection or access control bypass. The CRLF header acceptance is fixed in versions 2.1.13 and 2.2.2-alpha, but the reviewed patches do not clearly remediate the URI NUL-truncation condition.

CVE-2026-63387 - Libevent is an event notification library. Prior to 2.1.13 and 2.2.2-alpha, libevent has an off-by-one stack buffer overflow in evdns.c when dnsname_to_labels formats a name-bearing DNS record at the end of the 64 KB stack buffer allocated by evdns_server_request_format_response. The final-label check permits j plus label_len plus one to equal buf_len, after which the terminating null byte is written to buf[buf_len]. A crafted DNS server response containing PTR, CNAME, MX, NS, or SOA data can trigger the one-byte out-of-bounds write and crash or corrupt the process. This issue is fixed in versions 2.1.13 and 2.2.2-alpha.

CVE-2026-63388 - Libevent is an event notification library. Prior to 2.1.13 and 2.2.2-alpha, libevent has a heap out-of-bounds write in bufferevent_sock.c when bufferevent_socket_set_conn_address_ copies a kernel-supplied AF_UNIX peer address into bufferevent_private.conn_address. Release builds compiled with NDEBUG disable the EVUTIL_ASSERT length guard, and the evhttp accept path can pass a 110-byte sockaddr from accept() into the 28-byte field. An unauthenticated local peer able to connect to an AF_UNIX listener can overwrite the adjacent dns_request pointer and heap

IBM Champion
2022
IBM

data, causing memory corruption with confidentiality, integrity, and availability impact. This issue is fixed in versions 2.1.13 and 2.2.2-alpha.

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:

key_fileset = aix

For NTP:

Fileset	Lower Level	Upper Level	KEY	PRODUCT(S)
ntp.rte	7.4.2.8100	7.4.2.8172	key_w_fs	NTP
ntp.rte	73.4.2.8151	73.4.2.8172	key_w_fs	NTP

For tmux:

Fileset	Lower Level	Upper Level	KEY	PRODUCT(S)
tmux.rte	3.5.1.0	3.5.1.0	key_w_fs	tmux

Link

- **Vulnerabilities in libxml2 (CVE-2026-86140, CVE-2026-86141, CVE-2026-86143, CVE-2026-86144) affect AIX.**
  Vulnerabilities in libxml2 could cause stack-based buffer overflow (CVE-2026-86140), A NULL pointer dereference (CVE-2026-86141), An integer overflow (CVE-2026-86143), denial-of-service (CVE-2026-86144). AIX uses libxml2 as part of its XML parsing functions.
  Vulnerability Details
  CVE-2026-86140 - In libxml2 before 2.15.4, xmlSnprintfElements in valid.c has a strcat stack-based buffer overflow.
  CVE-2026-86141 - xmlregexp in libxml2 before 2.15.4 has a NULL pointer dereference in xmlRegNewParserCtxt after a strdup failure, i.e., it does not calculate a string length after NULL checking.
  CVE-2026-86143 - In xmlIO in libxml2 before 2.15.4, an inconsistency in xmlOutputWriteCallback and xmlBufUse causes negative lengths to reach write callbacks, aka a lack of a check for integer overflow before calling writecallback. This has security relevance for many types of uses of that length value within a callback.
  CVE-2026-86144 - In xinclude in libxml2 before 2.15.4, xmlXIncludeProcess and xmlXIncludeProcessTree do not propagate parseFlags. This has security relevance for, for example, the XML_PARSE_NONET flag, if (without it) a custom resource loader accesses the internet and triggers XML external entity injection, SSRF, or a denial of service (e.g., for an attacker-controlled internet resource that is intentionally slow).

IBM Champion
2022
IBM

Affected Products and Versions

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

The following fileset levels are vulnerable:

key_fileset = aix

Fileset	Lower Level	Upper Level	KEY
bos.rte.control	7.2.5.0 7	.2.5.208	key_w_fs
bos.rte.control	7.3.2.0	7.3.2.4	key_w_fs
bos.rte.control	7.3.3.0	7.3.3.3	key_w_fs
bos.rte.control	7.3.4.0	7.3.4.2	key_w_fs

Link

- **Multiple vulnerabilities in Python affect AIX**
  Vulnerabilities in Python: SSL/TLS Security Vulnerabilities (CVE-2026-19553, CVE-2026-19445), Archive Extraction / Tarfile Vulnerabilities (CVE-2026-19672, CVE-2026-82049, CVE-2026-87910), Authentication / Credential Exposure (CVE-2026-15806), Memory Management Vulnerabilities (CVE-2026-15310, CVE-2026-102633, CVE-2026-77214), Unicode / Encoding Issues (CVE-2026-93990, CVE-2026-17084). Python is used by AIX as part of Ansible node management automation.
  Vulnerability Details
  CVE-2026-19553 - ssl.SSLContext.wrap_bio() didn't require the server_hostname argument to not be None if ssl.SSLContext.check_hostname was set. Due to a missing parameter check in SSLObject, if the server_hostname argument isn't supplied then hostname verification would be silently skipped. This defect could lead to programs where certificate hostname verification *appeared* to be succeeding with SSLContext.check_hostname = True and no ValueError being raised due to misconfiguration. If the program passes a server_hostname value that isn't an empty string or None to any of these APIs then certificate hostname verification proceeds as expected and the program is not affected by this vulnerability. Mitigating this vulnerability doesn't require updating Python or applying the patch. To mitigate, pass a valid non-None and non-empty server_hostname value to SSLContext.wrap_bio(), asyncio.create_connection(), or asyncio.loop.start_tls() and certificate hostname verification will proceed as expected. Upgrading to the latest version of Python or applying the patch only changes the behavior from silently skipping hostname verification to raising a ValueError, similar to SSLContext.wrap_socket(), when server_hostname isn't supplied.
  CVE-2026-15310 - When decompressing crafted zip files using the bzip/LZMA/Zstandard compressions, Python could use an attacker-controlled size to pre-allocate memory, possibly resulting in memory exhaustion.

IBM Champion
2022
IBM

CVE-2026-19672 - The tarfile module's tar and data extraction filters created directories outside the destination for members whose name leaves the destination and returns to it, such as ../evil/../dest/sub/file. The containment check used the resolved path, but intermediate directories were created from the name as given. Only empty directories are created outside the destination. Member contents are still extracted inside it. To return to the destination the member's name must contain the destination directory's own final component, so extraction into a secure randomised directory is not affected. This affects POSIX platforms only. On Windows, .. components are collapsed before the path reaches the filesystem, so the directories outside the destination are never created.

CVE-2026-15806 - The HTTPPasswordMgr class in the urllib.request module, along with its subclasses HTTPPasswordMgrWithDefaultRealm and HTTPPasswordMgrWithPriorAuth, did not take the URL scheme into account when matching stored credentials against a requested URL. Credentials added for an https:// URL were also used for requests to the same host over http://, so an attacker able to redirect or downgrade a client to plain HTTP (for example, via an HTTPS-to-HTTP redirect or an on-path position) could capture credentials in cleartext. Credentials added for http:// URLs could likewise be sent over https://. Credential matching is now scoped by URL scheme. Credentials registered with a URL that includes a scheme are only used for requests with the same scheme. Credentials registered with a bare authority (such as example.com or example.com:8080) continue to match any scheme, preserving compatibility with existing code, including proxy authentication. Users who cannot upgrade immediately can mitigate by ensuring that applications never make plain http:// requests to hosts for which credentials are registered, for example by not following redirects to http:// URLs.

CVE-2026-17084 - The "stringprep" module didn't process characters from RFC 3454 tables B.2 or B.3 correctly: the latest Unicode codepoint attributes were used instead of the specified Unicode 3.2.0. This behavior would cause mismatches when processing domain names using IDNA 2003 (the "idna" codec) and the in_table_b2() function of the "stringprep" module. This only affects domain names containing characters that were not previously registered or had their Unicode attributes such as case-folding behavior updated since Unicode 3.2.0.

CVE-2026-102633 - libexpat versions 2.7.2 through 2.8.5 contain an integer overflow vulnerability in expat_realloc() function on 32-bit platforms when computing allocation sizes. Attackers supplying malicious XML to applications parsing with vulnerable libexpat can cause heap buffer overflow, memory corruption, or denial of service.

CVE-2026-82049 - In CPython 3.13 and earlier, the tarfile module's data and tar extraction filters are vulnerable to crafted archives containing a hard link to a symbolic link. Such archives may cause extraction to modify the permissions

IBM Champion
2022
IBM

or modification time of a file outside the destination directory, or expose the contents of that file within the extracted tree.

CVE-2026-87910 - When tarfile extracts a link on a system that doesn't support links, it falls back to extracting a member from the archive. In this case, the filter function is run twice: once for the extracted member, and once with name set to the location of the link. For one of the calls, the return value was ignored. Instead, the member should be skipped if either call returns None.

CVE-2026-93990 - Expat before 2.8.5 fails to validate that a high surrogate in UTF-16 input is followed by a low surrogate, allowing malformed UTF-16 sequences to be accepted. Attackers can supply UTF-16 encoded XML containing lone high surrogates that consume the following code unit, causing Expat to pass unpaired surrogates to applications built with XML_UNICODE and to silently replace input characters in other builds.

CVE-2026-19445 - A remote, unauthenticated TLS client can make a server crash or call through a freed pointer if its sni_callback assigns a different context to SSLSocket.context (the documented way to select a certificate per server name) and nothing else keeps the original ssl.SSLContext alive. Typical cases are servers that create an SSLContext per connection or replace it while connections are open; servers that wrap their listening socket with it are not affected. Mitigation: keep a reference to every SSLContext that sets sni_callback for the lifetime of the server. TLS clients are not affected.

CVE-2026-77214 - libexpat before commit 13c5f63 contains a heap buffer over-read vulnerability in xmlparse.c. XML_ParseBuffer advances the parse buffer end with parser-m_bufferEnd += len using a caller-supplied length that is not validated against the allocated buffer size, so repeated XML_ParseBuffer calls move m_bufferEnd past the end of the heap allocation and subsequent parsing reads out of bounds. Reaching this path requires a parse buffer to already be present; otherwise XML_ParseBuffer returns XML_ERROR_NO_BUFFER. A buffer is present after a prior call to XML_GetBuffer, either directly (the common case) or indirectly through a prior XML_Parse call that allocates the buffer internally. The over-read discloses adjacent heap memory to the calling application, recovering heap pointers, libc function pointers, and code pointers sufficient to defeat ASLR and build further exploitation primitives.

Affected Products and Versions

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

IBM Champion
2022
IBM

The vulnerabilities in the following filesets are being addressed:

key_fileset = osrcaix

Fileset	Lower Level	Upper Level	KEY
python3.9.base	3.9.0.0	3.9.24.0	key_w_fs
python3.11.base	3.11.0.0	3.11.16.0	key_w_fs
python3.14.base	3.14.0.0	3.14.7.0	key_w_fs

Link

- **Multiple vulnerabilities in IBM Java SDK affect AIX**
  There are multiple vulnerabilities in IBM SDK Java Technology Edition,Version 8 used by AIX. AIX has addressed the applicable CVEs.
  Vulnerability Details
  CVE-2026-61308 - Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Java SE. While the vulnerability is in Java SE attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE accessible data.
  CVE-2026-70907 - Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE.
  CVE-2026-60589 - Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data.
  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:

  key_fileset = java

Fileset	Lower Level	Upper Level	Level KEY
Java8.jre	8.0.0.0	8.0.0.870	key_w_fs
Java8.sdk	8.0.0.0	8.0.0.870	key_w_fs
Java8_64.jre	8.0.0.0	8.0.0.870	key_w_fs
Java8_64.sdk	8.0.0.0	8.0.0.870	key_w_fs

  Link

- **Multiple vulnerabilities impacts AIX due to cURL libcurl.**
  Multiple vulnerabilities in the curl/libcurl are related to input validation flaws (CVE-2026-13608), memory corruption (CVE-2026-18924), information disclosure (CVE-2026-19931), denial of service (CVE-2026-80230), privilege escalation (CVE-2026-80231), and security policy bypass (CVE-2026-82209).

IBM Champion
2022
IBM

Vulnerability Details

CVE-2026-13608 - A flaw in the libcurl SASL negotiation for LDAP authentication allows an incomplete handshake sequence to be misinterpreted as a successful cryptographic verification. An attacker executing a Man-in-the-Middle (MITM) attack can inject a premature or shortcut response that bypasses complete peer validation.

CVE-2026-18924 - A flaw in libcurl's handling of HTTP/2 Server Push streams, when the parent handle is set to share connections with other handles, can lead to use-after-free in the cleanup process.

CVE-2026-19931 - A flaw in libcurl makes it wrongly reuse an HTTP connection setup for a given hostname using Negotiate authentication, when the initial request is done using empty credentials. This can make user B's request get sent over user A's previously authenticated connection.

CVE-2026-80230 - When `CURLOPT_PINNEDPUBLICKEY` is configured alongside options that disable standard peer verification (`CURLOPT_SSL_VERIFYPEER = 0` and `CURLOPT_SSL_VERIFYHOST = 0`), libcurl fails to enforce public key pinning on connections established without a presented server certificate. Bypassing the pinning check under these disabled-verification conditions allows unauthenticated connections to succeed when they should be rejected.

CVE-2026-80231 - A flaw in libcurl makes it wrongly reuse an existing HTTPS connection setup for a given hostname even when using a different Native CA Store setting (`CURLSSLOPT_NATIVE_CA`) than when the connection was created.

CVE-2026-82209 - When libpsl support is enabled, libcurl fails to enforce the Public Suffix List boundary check when processing a `Set-Cookie` header where the `Domain` attribute explicitly matches an origin host that is itself a public suffix (e.g., `Domain=co.uk` set by `co.uk`). Instead of coercing it into a strict host-only cookie, libcurl saves the cookie with wildcard domain scope (`.co.uk`). Consequently, the cookie is inappropriately included in subsequent outbound requests or HTTP redirects to arbitrary sibling subdomains under the same public suffix (e.g., `attacker.co.uk`).

Affected Products and Versions

Affected Product(s)	Version(s)
AIX	7.3

The following fileset levels are vulnerable:

key_fileset = aix

Fileset	Lower Level	Upper Level	KEY
oss.lib.libcurl	7.79.1.0	7.79.1.0	key_w_fs
oss.lib.libcurl	8.1.2.0	8.1.2.0	key_w_fs
oss.lib.libcurl	8.5.0.0	8.5.0.2	key_w_fs

Link

IBM Champion
2022
IBM

GPFS/Scale HIPER:

- **IBM Storage Scale may experience undetected data loss or corruption when it reads from loop-mounted images that are stored in IBM Storage Scale on newer Linux kernels**

  Risk categories

  Data Loss

  Affected Domain

  Users may be affected if they read from or write to loop devices whose backing files reside on an IBM Storage Scale file system running a Linux kernel that contains the following commit:

  f2fed441c69b ("loop: stop using vfs_iter_{read,write} for buffered I/O")

  This commit was included in the upstream Linux kernel, starting with 6.15. And the commit has also been backported to several distribution kernels, including:

  Red Hat: kernel 5.14.00597
  SLES: kernel 6.4.001507005306
  Ubuntu: kernel 6.14.04000

  Affected versions of IBM Storage Scale need a fix.

  - Users that run IBM Storage Scale 5.2.3.0 through 5.2.3.9 should upgrade to IBM Storage Scale 5.2.3.10 or later
  - Users that run IBM Storage Scale 6.0.0.0 through 6.0.1.1 should upgrade to IBM Storage Scale 6.0.1.2 or later
  - If an upgrade to a release with the fix can not be performed, request an interim fix (efix) via APAR IJ60020.

  Link

GPFS/Scale alerts:

- **IBM Storage Scale: Kernel crash during mmstartup run due to missing IBT support**

  Abstract

  IBM Storage Scale versions 6.0.0.0 - 6.0.1.2 may encounter a kernel panic and system restart when mmstartup is run on RHEL 10 (kernel 6.12.x) with IBT-capable Intel CPUs. The mmfs26 kernel module is built without the IBT support that is required by Intel's hardware-enforced Control-Flow Integrity (CET/IBT), which causes the CPU to raise a #CP (Control Protection fault) on module load.

  Problem Description

  When the mmstartup command runs on nodes with RHEL 10.0 or 10.1 or 10.2, in combination with IBT-capable Intel CPUs, the command execution can cause an immediate kernel panic and a system restart.

  Technical Details

IBM Champion
2022
IBM

The mmfs26 kernel module is built without IBT support. On IBT-enabled hardware, every indirectly called function must begin with ENDBR64. When insmod loads mmfs26, the CPU finds 0x55 (push rbp) instead of ENDBR64 at init_module+0x0, which immediately triggers a fatal #CP fault (see the following example).

```
RIP: 0010:init_module+0x0/0xb0 [mmfs26]
Code: ... <55> 48 89 e5 ...
```

Affected Versions

IBM Storage Scale versions: 6.0.0.0 - 6.0.1.2
Operating sytem: Linux RHEL 10.0, 10.1, 10.2 (kernel 6.12.x)
Hardware: Physical servers with IBT-capable Intel CPUs

Symptoms

System restart occurs immediately after mmstartup runs.
New entry is created under /var/crash/ after each attempt.
Kernel panic that shows exc_control_protection with RIP: init_module+0x0/0xb0 [mmfs26]
SSH session into that node drops with "Operation timed out".

Workaround

- Disable IBT through the kernel boot parameter by following the next steps:
- Edit /etc/default/grub to append ibt=off to GRUB_CMDLINE_LINUX_DEFAULT
- Regenerate the GRUB configuration: grub2-mkconfig -o /boot/grub2/grub.cfg
- Reboot the system.

Link

- **The following vulnerabilities that can affect IBM Storage Scale and the Samba Cluster Export Services (CES) layer are now addressed in 6.0.1.2 or higher**

The following vulnerabilities, which can affect IBM Storage Scale and the Samba Cluster Export Services (CES) layer and could provide weaker-than-expected security, are now addressed in Storage Scale 6.0.1.2 or higher.

Vulnerability Details

CVE-2026-58216 - An out-of-bounds read flaw was found in Samba's Kerberos Key Distribution Center's (KDC) password change (kpasswd) service. When processing malformed ASN.1-encoded Kerberos password change request, Samba server miscalculates the structure size and attempts to read up to six bytes beyond the end of the allocated buffer. While this out-of-bounds read typically results in a harmless decryption failure, if the read hits unmapped memory, it causes the KDC process to crash. An authenticated attacker can send a specially crafted kpasswd request containing malformed ASN.1 data to trigger the out-of-bounds read, which may cause the KDC process to terminate, resulting in a denial of service.

CVE-2026-58218 - A flaw was found in Samba's internal DNS server where unauthenticated TKEY registration requests were added to the TKEY name

IBM Champion
2022
IBM

cache before being rejected. A remote, unauthenticated attacker can exploit this behavior by sending a large number of TKEY requests with arbitrary names, exhausting the cache and evicting legitimate TKEY entries. This can prevent legitimate TSIG authentication for signed DNS queries, resulting in a denial of service.

CVE-2026-58222 - A security flaw combining LDAP filter injection and improper authorization checks was found in Samba Active Directory Domain Controller (AD DC). When processing LDAP Compare requests, Samba fails to properly validate user-supplied attribute names and executes the resulting internal database search in a trusted context, bypassing normal Access Control List (ACL) enforcement. An authenticated low-privilege domain user can exploit these flaws to disclose confidential Active Directory attributes that would normally be inaccessible. The disclosed information may be leveraged to derive sensitive authentication material, potentially leading to privilege escalation and complete domain compromise. For example: In deployments configured with Group Managed Service Accounts (gMSAs), an attacker can extract the "msKds-RootKeyData" attribute and derive gMSA passwords offline, potentially leading to complete domain compromise if privileged gMSAs are present.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale	IBM Storage Scale 6.0.0.0 - 6.0.1.1

Remediation/Fixes

For IBM Storage Scale 6.0.x, IBM strongly recommends addressing the vulnerability by upgrading to 6.0.1.2 or later:

Link

- **The following vulnerabilities that can affect IBM Storage Scale System and the Management GUI are now fixed in 6.2.3.6 or higher and 7.0.1.1 or higher**

The following vulnerabilities, which can affect IBM Storage Scale System and the Management GUI and could provide weaker-than-expected security, are now fixed in Storage Scale 6.2.3.6 or higher and 7.0.1.1 or higher.

Vulnerability Details

CVE-2026-13460 - IBM Storage Scale 5.2.3.0 through 5.2.3.8, and 6.0.0.0 through 6.0.1.0 GUI contains a hardcoded token in the source code, which was used for inter-node cluster communication and REST API authentication between GUI.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale System	6.2.3.0 - 6.2.3.5
IBM Storage Scale System	7.0.0.0 - 7.0.1.0

Remediation/Fixes

For IBM Storage Scale 6.2.3.x, IBM strongly recommends addressing the vulnerability by upgrading to 6.2.3.6 or later:

IBM Champion
2022
IBM

Link

Some other AIX/PowerVM fixes:

- Multiple vulnerabilities in rpm.rte affect AIX (7.2/7.3 and VIO 4.1).
  Link
- A heap buffer overflow vulnerability in rsyslog impacts AIX (7.2/7.3 and VIO 4.1).
  Link
- Multiple vulnerabilities in PostgreSQL affect PowerVM VIOS 4.1
  Link

Some other GPFS/Scale fixes:

- FIFO (named pipe) read/write hangs on nodes that run IBM Storage Scale 5.2.3.8 - 5.2.3.9 and 6.0.1.0 - 6.0.1.1
  Link
- IBM Storage Scale 6.0.1.0 - 6.0.1.1 and IBM Storage Scale System 7.0.1.0: File systems with DMAPI fail to mount on remote cluster nodes
  Link
- The following vulnerabilities that can affect IBM Storage Scale native REST API are now fixed in 5.2.3.10 or higher and 6.0.1.2 or higher
  Link
- The following vulnerabilities that can affect IBM Storage Scale cloudkit are now fixed in 5.2.3.10 or higher and 6.0.1.2 or higher
  Link
- The following vulnerabilities that can affect IBM Storage Scale and the Samba Cluster Export Services (CES) layer are now addressed in 6.0.1.2 or higher
  Link
- IBM has identified issues affecting Active File Management (AFM) in IBM Storage Scale 5.2.3.0 - 5.2.3.9 or 6.0.0.0 - 6.0.1.1 that may result in undetected data corruption or data loss
  Link

Keep safe and keep Power-ing on!
Red, Belisama

IBM Champion
2022
IBM