Belisama

December Newsletter

Subscribe/Unsubscribe

Greetings all,
Wishing you all the best for a successful end of ‘24 and a great start to ‘25

A few updates to share

- See the IBM Champions at Las Vegas
- Future Power processors – quick read from Timothy Morgan, who was surprised that IBM didn’t announce the new Power11 details at Hot Chips or TechXchange – but shared the latest details here (including the new Spyre adapter) – Link
- Wade Tyler Millward on the Power11 Release: ‘It’s More Tools In Our Partners’ Belts’ – Link
- Andrey has more insights in his automation journey – and easy ways spoil your Security team (which we know will keep everyone else happy) - Link

Quick bites

NIM Network ports
Support has published a quick Technote on the ports used by NIM communications. Answers the common question “How can I configure my switches, routers, gateways, firewalls, etc., to allow for NIM operations requiring network communication between a NIM master and it's clients, to complete successfully?”
Link

PowerVM Virtual I/O Server
In case you missed it, a Shared Ethernet Adapter no longer requires a dedicated control channel adapter. How to simplify our PowerVM configuration.
What is the prerequisite to use this feature?
VIOS level 2.2.3.0 and higher.
System firmware level 7.8 and higher.
Link

Upgrading Your Storage Scale Cluster, Part 2
Another beautifully presented article from IBM Champion Jaqui Lynch. The second part where she shares the lessons she learned when upgrading from Spectrum Scale 5.1.7.1
Link

Of Dials and Switches: An Introduction to Tuning the AIX Kernel
The kernel is the heart of any operating system. A major function of this core code is to provide access to the hardware on which it runs. Mark J. Ray has frequently written about tuning AIX, but now digs a bit deeper.
Link

Redbooks and Redpapers

- **IBM Power E1050 Technical Overview and Introduction**, Redpaper, revised 21 November 2024
  Link
- **IBM Power E1080 Technical Overview and Introduction**Redpaper, revised 16 November 2024
  Link
- **IBM Power Security Catalog**, Draft Redbook, published 16 November 2024
  Link
- **Accelerating AI and Analytics with IBM watsonx.data and IBM Storage Scale**, Redpaper, published 15 November 2024
  Link
- **Creating OpenShift Multiple Architecture Clusters with IBM Power**, Redbook, revised 14 November 2024
  Link

- **Using Ansible for Automation in IBM Power Environments**, Rebook, published 12 November 2024
  Link

IBM alerts and notices

AIX and PowerVM / Virtual I/O Server alerts

- **Security bulletin: Security Bulletin: AIX is vulnerable to a denial of service due to ISC BIND**

  Multiple vulnerabilities in ISC BIND could allow a remote attacker to cause a denial of service (CVE-2024-0760, CVE-2024-1737, CVE-2024-4076, CVE-2024-1975). AIX uses ISC BIND as part of its DNS functions.

  Vulnerability Details

  CVE-2024-0760 - ISC BIND is vulnerable to a denial of service. By sending a flood of DNS messages over TCP, a remote attacker could exploit this vulnerability to cause the server to become unstable.

  CVE-2024-1737 - ISC BIND is vulnerable to a denial of service, caused by an error when content is being added or updated in resolver caches and authoritative zone databases that hold significant numbers of RRs for the same hostname (of any RTYPE). By processing queries, a remote attacker could exploit this vulnerability to cause the database to slow down.

  CVE-2024-4076 - ISC BIND is vulnerable to a denial of service, caused by an error when serving both stale cache data and authoritative zone content. By sending queries, a remote attacker could exploit this vulnerability to cause an assertion failure.

  CVE-2024-1975 - ISC BIND is vulnerable to a denial of service, caused by an error if a server hosts a zone containing a "KEY" Resource Record, or a

resolver DNSSEC-validates a "KEY" Resource Record from a DNSSEC-signed domain in cache. By sending a stream of SIG(0) signed requests, a remote attacker could exploit this vulnerability to exhaust all available CPU resources.

Affected Products

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

The following fileset levels are vulnerable:

Fileset	Lower Level	Upper Level
bind.rte	7.1.916.0	7.1.916.4800
bind.rte	7.2.916.0	7.2.916.4801
bind.rte	7.3.916.0	7.3.916.4800

Link

- **Security bulletin: Security Bulletin: AIX is vulnerable to arbitrary command execution due to invscout (CVE-2024-47115)**

A vulnerability in the AIX invscout command could allow a non-privileged local user to execute arbitrary commands (CVE-2024-47115).

Vulnerability Details

CVE-2024-47115 - IBM AIX could allow a local user to execute arbitrary commands on the system due to improper neutralization of input.
CWE: CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Affected Products and Versions

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

The following fileset levels are vulnerable:

Fileset	Lower Level	Upper Level
invscout.rte	2.2.0.0	2.2.0.26

Link

- **Security Bulletin: AIX is affected by multiple vulnerabilities due to Python**

There are multiple vulnerabilities in Python used by AIX (CVE-2024-45491, CVE-2024-45490, CVE-2024-45492, CVE-2024-7592, CVE-2024-8088, CVE-2024-6923). Python is used by AIX as part of Ansible node management automation.

Vulnerability Details

CVE-2024-45491 - libexpat could allow a local attacker to execute arbitrary code on the system, caused by an integer overflow in the dtdCopy function in xmlparse.c. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary code on the system.
CVE-2024-45490 - libexpat could provide weaker than expected security, caused by not reject a negative length for XML_ParseBuffer. A local attacker could exploit this vulnerability to launch further attacks on the system.

CVE-2024-45492 - libexpat could allow a local attacker to execute arbitrary code on the system, caused by an integer overflow in the nextScaffoldPart function in xmlparse.c. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary code on the system.
CVE-2024-7592 - Python CPython is vulnerable to a denial of service, caused by improper input validation by the http.cookies._unquote() function. By parsing specially crafted cookies that contained backslashes for quoted characters in the cookie value, a remote attacker could exploit this vulnerability to use excess CPU resources.
CVE-2024-8088 - Python CPython is vulnerable to a denial of service, caused by an infinite loop flaw when iterating over names of entries in a zip archive. By using a specially crafted zip archive, a remote attacker could exploit this vulnerability to cause a denial of service condition.
CVE-2024-6923 - Python CPython is vulnerable to email header injection, caused by the failure to properly quote newlines for email headers when serializing an email message. By persuading a victim to open a specially crafted email, a remote authenticated attacker could exploit this vulnerability to spoof sender identity, gain unauthorized email sending or loss of control over email communication.

Affected Products and Versions

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

The following fileset levels are vulnerable:

Fileset	Lower Level	Upper Level
python3.9.base	3.9.0.0	3.9.19.3

Link

- **Security Bulletin: AIX is vulnerable to arbitrary code execution (CVE-2023-36328) due to tcl**

Vulnerability in tcl could allow a remote attacker to execute arbitrary code or cause a denial of service (CVE-2023-36328).

Vulnerability Details

CVE-2023-36328 - libtom libtommath is vulnerable to an integer buffer overflow, caused by improper bounds checking by mp_grow. By sending a specially crafted request, a remote attacker could overflow a buffer and execute arbitrary code and cause a denial of service.

Affected Products and Versions

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

The following fileset levels are vulnerable:

Fileset	Lower Level	Upper Level

tcl.base 8.6.10.0 8.6.10.0

Link

- **Security Bulletin: 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-2024-21145 - An unspecified vulnerability in Java SE related to the 2D component could allow a remote attacker to cause low confidentiality, low integrity impacts.

CVE-2024-21144 - An unspecified vulnerability in Java SE related to the Concurrency component could allow a remote attacker to cause low availability impact.

CVE-2024-21131 - An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause low integrity impact.

CVE-2024-27267 - The Object Request Broker (ORB) in IBM SDK, Java Technology Edition 7.1.0.0 through 7.1.5.18 and 8.0.0.0 through 8.0.8.26 is vulnerable to remote denial of service, caused by a race condition in the management of ORB listener threads. IBM X-Force ID: 284573.

Affected Products and Versions

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

The following fileset levels (VRMF) are vulnerable, if the respective Java version is installed:

For Java8: Less than 8.0.0.830

Link

AIX alerts / Problem solving information:

- **IJ52978: A POTENTIAL SECURITY ISSUE EXISTS**

This APAR addresses a potential security issue. Any relevant information will be released via My Notifications.

Link

- **IJ52967: LOGS IN ASO TO CAPTURE REASON FOR UNSUCCESSFUL SHM PROMOTIONS**

ASO promotes the SHM pages that it finds to be hot to 16MB.
Currently, we do not capture the reason if the pages do
not get promoted.

Link

- **IJ52955: VMSTAT OUTPUT FI/FO SEEMS INCORRECT WHEN SYSTEM IS IN A PAGING**

Output values jump from 0 to huge number

Link

- **IJ52977: A POTENTIAL SECURITY ISSUE EXISTS**
  This APAR addresses a potential security issue. Any relevant information will be released via My Notifications.
  Link
- **J52943 / IJ52962: JAVA 21: PROBLEM EXTRACTING FILES FROM JAR/ZIP WITH NX/GZIP**
  When using the GZIP accelerator on Power 9 and Power 10 Java 21 Semeru cannot find classes that are greater than 1KB.
  The problem is that when the zip entry is uncompressed using zlibNX only the first 1024 bytes of uncompressed data are returned.
  Then the method jdk.internal.loader.Resource.getBytes throws an EOFException with the message "Detect premature EOF".
  Local fix
  Disable gzip accelerator for an application by setting this environment variable:
  # export ZLIB_DECOMPRESS_ACCEL=0
  Link and Link
- **IJ52942/IJ52973: SGID NOT PRESERVED WHEN IFIX IS INSTALLED IN NIMADM**
  Some files replaced by an ifix installed via NIMADM may loose their SGID or SUID.
  Local fix
  Manually add the missing permission post migration or install the ifix post NIMADM.
  Link and Link
- **IJ52964: DUMPLV NT ENCR FREE SLT AVLBLE**
  If hd7 already exists before starting the installation, the user won't be able to encrypt or decrypt the traditional sysdump device (hd7) during a preservation or migration installation.
  Link
- **IJ52952: LKU ON PVC DOES NOT REMOVE TEMP PAGING SPACE FROM CFG FILE**
  PowerVC managed Live update will not remove the temporary paging space disk stanza from the liveupdate.cf file. This leads to clvupdate reporting a failed cleanup even in a clean system.
  Local fix
  Remove disk url and wwn from liveupdate.cf file.
  Link
- **IJ52974: SYSTEM ASSERT WHEN WRONG SEGMENT PASSED DURING MEMORY MIGRATION**
  During migration of shared memory regions of a user application by ASO, if a wrong argument is passed by ASO, system can crash.
  Link

- **IJ52951: INCOMPLETE OUTPUT BY "MALLOC ALLOCATION SIZE==X" COMMAND IN DBX**
  dbx command "malloc allocation" is not reporting complete list of allocations when specifically called to display allocations of a particular size using the option size==XX.
  The issue is observed when using the following sub command within the dbx session "malloc allocation size==xx" otherwise, it will display all the allocations without any issue.
  Link
- **IJ52972: PASSIVE VG FAILS TO VARYON AFTER LKU WITH POWERHA**
  liveupdate of an lpar running PowerHA with concurrent Vgs in passive mode will leave those VGs offline after liveupdate.
  Link
- **IJ52960: HST 1060.20 SP: INACTIVE LPM IS FAILING FOR NPIV LPAR WITH HSC**
  INACTIVE_LPM from vios version 72Z or 73D to 73F will fail
  Link
    - **IJ52971: ISST:AUS:MAYUR09:LI-094:PRESERVE UPDATE NOT KEEPING THE CONFIGURATION**

  If hd7 is created as dumplv, it will not be encrypted during a preservation installation, even if the user selects "yes" in the BosMenus - Select LVs for Encryption menu or uses a non-prompt method. If the user chooses "preserve" for the LV in the BosMenus - Select LVs for Encryption menu or uses a non-prompt method and the LV is locked, encryption will not be applied to the LV.
  Link
- **IJ52959: IO FAILS ON VFC PATH, AFTER EEH ON 8GB OLDER ADAPTER**
  IO fails on VFC adapter
  Link
- **IJ52958: VIOS/AIX BOOT MAY HANG DURING BROADCOM FC HBA CONFIG**
  VIOS/AIX boot may hang while configuring the Broadcom FC HBA that has data rates equal to or more than 16Gb
  Link
- **IJ52947: LOGS IN ASO TO CAPTURE REASON FOR UNSUCCESSFUL SHM PROMOTIONS**
  ASO promotes the SHM pages that it finds to be hot to 16MB. Currently, we do not capture the reason if the pages do not get promoted.
  Link
- **IJ52968: INSTFIX FAILS TO LIST EFIXES WITH ABSTRACTS LONGER THAN 64**
  When an efix is installed via emgre with an abstract text that is longer than 64 chars instfix will fail to list it.
  Link
- **IJ53109: LKU WITH AUTOFS HANGS AT "MOVING WORKLOAD"**

Live update with autofs configured my hang during "Moving workload" stage.
Link

- **IJ53148: POTENTIAL CRASH IN BERKLEY PACKET FILTER (BPF) DRIVER**
  Data Storage Interrupt (invalid page fault) with following stack (partial):
  pvthread+093200 STACK:
  [0000F45C]___memmove64+00005C
  [005B85E4]_m_copym_base+000804
  [F10009D5B0486B38]bpf:process_ipv4_options+000058
  [F10009D5B0486FB8]bpf:inp_match+000178
  [F10009D5B0485644]bpf:bpf_aix_mtap+0002A4
  [00014D70].hkey_legacy_gate+00004C ()
  [F10009D5A053BC34]vioentdd:IPRA.$vioent_output_old+003034
  ... ...
  Link
- **IJ53049: PERFORMANCE DEGRADATION WITH JFS2 SNAPSHOT**
  Performance degradation when doing cached IOs on JFS2 snapshot
  Link
- **IJ53047: SHUTDOWN REPORTS FAILURES DUE TO /DEV/CONSOLE NOT AVAILABLE**
  The shutdown command reports failures due to /dev/console not available:
  /usr/sbin/shutdown[1376]: echo: write to 1 failed
  [There is an input or output error.]
  Link
- **IJ53056: EMGR_SEC_PATCH MAY FAIL TO INSTALL IFIX**
  The emgr_sec_patch may fail with below errors:
  Advisory.asc integrity verification passed
  ERROR: 98812360ee802af2f3a25de73479067448cd7dc1bc6887e
  06d5cafdf3f849c4e is not found in the tar file
  Link
- **IJ53043: FIND COMMAND MIGHT NOT WORK DUE TO MOUNT PERMISSIONS**
  The find command may report invalid directory due to mount permissions.
  Link
- **IJ53052: DUPLICATE UDP SOCKETS CAN GET CREATED CAUSING CONNECTION ISSUES**
  The following may provide guidance on how to specify tablespaces when installing IWS 10.1 (MDM/DWC).
  https://www.ibm.com/docs/ja/workload-automation/10.1.0?topic=customizations-how-can-i-modify-tablespace
  Also, even if PATH set in the following item in configureDb.properties, it does not seem to be reflected properly.
  Link

- **IJ53079: BACKUPIOS CAN HANG WHEN THE STDERR IS BIGGER THAN 32K**
  backupios can hang if the underlying commands generate a lot of output.
  We have seen this happen if applications create/destroy lots of files in rootvg while savevg/mksysb is running, and we've also seen it when bootpkg cannot restore files to the SPOT due to permissions errors.
  Both of these situations cause lots of output to stderr which results in ioscli process and underlying command both stuck, hung indefinitely until killed.
  Link
- **IJ53073: GXT500: FAILS OR 185S IN DIAGNOSTICS**
  If this occurs, one of three things might happen:
  1. a local dma error is logged against the bluesea registers
  2. a switch context error is logged
  3. box crashes after executing the switch context test

  Link and Link
- **IJ53084: EXTENDLV WITH MIRROR POOLS MAY ALLOCATE PARTITIONS INCORRECTLY**
  When extending a logical volume with upper bound 1 and mirror pools enabled, the physical partition allocation could incorrectly use more than 1 physical volume.
  Link
- **IJ53081: VIOS MAY CRASH AT NPIV_INIT_CMD**
  VIOS may crash. System will be unavailable.
  Link
- **IJ53146: DUPLICATE UDP SOCKETS CAN GET CREATED CAUSING CONNECTION ISSUES**
  This issue was discovered in an Oracle RAC environment with HAIP configuration where this was leading to Oracle DB crashes.
  Problem summary
  Same ephemeral port may get allocated to multiple sockets when socket is created with IP_EXPAND_EPHEMERAL flag. This may cause data not to be delivered to the correct socket and may cause applications like oracle to misbehave. This may happen when an IP address is moved from one interface to another interface or when IP addresses of multiple interfaces are swapped
  Link
- **IJ53144: BACKUPIOS CAN HANG WHEN THE STDERR IS BIGGER THAN 32K**
  backupios can hang if the underlying commands generate a lot of output.
  We have seen this happen if applications create/destroy lots of files in rootvg while savevg/mksysb is running, and we've also seen it when bootpkg cannot restore files to the SPOT due to permissions errors.
  Both of these situations cause lots of output to stderr which results in ioscli process and underlying command both stuck, hung indefinitely until killed.
  Link

- **IJ53132: REORGVG TERMINATION MAY HANG THE PASSIVE NODE DURING FAILOVER**

Terminating(ctrl+c) reorgvg on a active PowerHA cluster node may cause the passive node to hang during failover.
Terminating(ctrl+c) reorgvg on a active PowerHA cluster node may cause the passive node to hang during failover.
Local fix

Reboot of hung node

Problem summary

Cleanup code in reorgvg fails to notify the remote node that the migration/sync is no longer running. If the remote node later attempts writes to the last partition that was being syncd, those writes get held up indefinitely in the LVM layer.

Link

- **IJ53143: MISSING -EXCLUDE FLAG IN BACKUPIOS HELP**

Running backupios without any flag or backupios -help doesn't show the -exclude flag
Error description
Running backupios without any flag or backupios -help doesn't show the -exclude flag that is reported in the man page and in the doc
Local fix

Use -exclude flag even if it's not reported in the help as it's properly accepted

Link

- **IJ53142: EIO ERRORS FOR LOCK REQUESTS DUE TO BAD_SEQID**

EIO errors for lock requests are seen due to a BAD_SEQID.
Lock of an NFS4 file can fail with EIO.
An iptrace would show the NFS4 client sending an all-zero stateID with a lock request, and getting a BAD_SEQID error from the server.
Link

- **IJ53130: A POTENTIAL SECURITY ISSUE EXISTS**

This APAR addresses a potential security issue. Any relevant information will be released via My Notifications.
Link

- **IJ53141: KERNEL ASSERT, IF VSID IS INVALID IN VM_ATTINFO**

if vm_attinfo is called with invalid vsid, the kernel will crash.
Link

- **IJ53140: FORCE UNMOUNT OF A J2 FILESYSTEM MAY TAKE LONGER UNDER NFS ENV**

Here is a scenario where the force unmount of a J2 filesystem was taking longer than expected:
Link

- **IJ53129: A POTENTIAL SECURITY ISSUE EXISTS**

This APAR addresses a potential security issue. Any relevant information will be released via My Notifications.

Link

- **IJ53117: FORCE UNMOUNT OF A J2 FILESYSTEM MAY TAKE LONGER UNDER NFS ENV**
  Here is a scenario where the force unmount of a J2 filesystem was taking longer than expected:
  Link
- **IJ53139: DEBUG INFO TO PRINT THE PROCESS TREE IN CASE OF CHECKPOINT FAIL**
  Link
- **IJ53138: SYSTEM CRASH IN SELPOLL()**
  System crash with following stack: (24)> f 6154
  Link
  IJ53147: EXTENDLV WITH MIRROR POOLS MAY ALLOCATE PARTITIONS INCORRECTLY

Mellanox alerts:

- **Mellanox 25G SN2410 Switch (3454-B8C) and Mellanox 1G EdgeCore Switch (3454-A3C)**
  Software: 436: Failed to collect status from resource manager | bmc@appliance://
  The record has been re-opened.
  Error reported:
  Title : BMC Configuration error
  Type : HW_NEEDS_ATTENTION
  Reason Code : 866
  BMC configuration error alert.
  Link

IBM i alerts:

- **Hot plug of U.2 NVMe devices has never been supported on IBM i.**
  IBM i has always required a service procedure to replace storage devices. If a U.2 NVMe device was hot swapped or replaced by accident (without using the documented procedures), there would be two possible courses of action to recover that do not require an IPL.
  Environment
  U.2 NVMe on IBM i supported systems
  Link

- **IBM i microcode**
  IBM i applies adapter microcode to adapters when the adapters are assigned to partitions and the adapters are activated. If the IBM i partition has older adapter microcode PTFs applied, this can push older adapter microcode to the adapter. Under most circumstances this is not a problem. In this specific case, Revision A5 or

later of the Feature Code EN24 / EN26 CCIN EC2A adapter (PCIe4 x16 4-port 25/10/1 GbE RoCE SFP28 adapter) does not support older adapter microcode. If IBM i pushes an older, unsupported, level to the adapter, configuration changes occur, the adapter will cease to function, and the adapter is not easily recoverable. Replacement of the adapter may be necessary.
Exposure Criteria:

Communications Adapter Feature Code EN24 / EN26 CCIN EC2A adapter (PCIe4 x16 4-port 25/10/1 GbE RoCE SFP28 adapter) at Revision A5 or later.

- IBM i 7.4:
  - Exposed: Resave ibase_01 RS-740-N marker RE23272 through RS-740-P marker RE24074
  - Exposed: Technology Refresh 7.4 TR9 through 7.4 TR11
- IBM i 7.5:
  - Exposed: Resave ibase_01 RS-750-D marker RE23277 through RS-750-E marker RE24122
  - Exposed: Technology Refresh 7.5 TR3 through 7.5 TR5

Link

PowerHA SystemMirror

- **Security Bulletin: PVR0501342 [Express - CVE-2024-29041 (Publicly disclosed vulnerability)]**

This Security Bulletin is created to reflect the remedian done for PVR0501342 [Express - CVE-2024-29041 (Publicly disclosed vulnerability). The 'express' has been upgraded in PowerHA GUI Rel 7.2.9 from version 4.16.4 to version 4.19.2 in order to resolve this PVR.
Vulnerability Details

CVE-2024-29041- Express.js Express could allow a remote attacker to conduct phishing attacks, caused by an open redirect vulnerability. An attacker could exploit this vulnerability using a specially crafted URL to redirect a victim to arbitrary Web sites.

Affected Products and Versions

Affected Product(s)	Version(s)
PowerHA	All

Remediation/Fixes

The 'express' has been upgraded in PowerHA GUI Rel 7.2.9 from version 4.16.4 to version 4.19.2 in order to resolve this PVR.

Link

- **Security Bulletin: PVR0546850 - Express - CVE-2024-45590 (Publicly disclosed vulnerability)**

This Security Bulletin is created to reflect the remedian done for PVR0546850 - Express - CVE-2024-45590 (Publicly disclosed vulnerability). The 'body_parser' has

been upgraded to version 1.20.3 in PowerHA GUI Rel 7.2.9 in order to resolve this PVR.
Vulnerability Details
CVE-2024-45590 - expressjs body-parser is vulnerable to a denial of service, caused by a flaw when url encoding is enabled. By sending a specially crafted payload, a remote attacker could exploit this vulnerability to cause a denial of service condition.
Affected Products and Versions

Affected Product(s)	Version(s)
PowerHA	All

Remediation/Fixes
The 'body_parser' has been upgraded to version 1.20.3 in PowerHA GUI Rel 7.2.9 in order to resolve PVR0546850 - Express - CVE-2024-45590 (Publicly disclosed vulnerability).
Link

PowerVC

- **Security Bulletin: User can inject the suspected code via URL passed**
  A vulnerability in the package_index module of pypa/setuptools versions up to 69.1.1 allows for remote code execution via its download functions. These functions, which are used to download packages from URLs provided by users or retrieved from package index servers, are susceptible to code injection. If these functions are exposed to user-controlled inputs, such as package URLs, they can execute arbitrary commands on the system.
  Vulnerability Details
  Refer to the security bulletin(s) listed in the Remediation/Fixes section
  Affected Products and Versions

Affected Product(s)	Version(s)
PowerVC	2.1.0, 2.1.1, 2.2.0, 2.2.1

  Remediation/Fixes
  Upgrade to the latest PowerVC version 2.2.1.1
  Link

- **Security Bulletin: PowerSC is vulnerable to information disclosure, denial of service, and security restrictions bypass due to Curl**
  Vulnerabilities in Curl could allow a local attacker to obtain sensitive information (CVE-2024-7264) or a remote attacker to cause a denial of service (CVE-2024-6197, CVE-2024-37371) or bypass security restrictions (CVE-2024-37370). PowerSC uses Curl as part of PowerSC Trusted Network Connect (TNC).
  Vulnerability Details
  CVE-2024-7264 - cURL libcurl could allow a local attacker to obtain sensitive information, caused by an out-of-bounds read flaw in the the GTime2str() function. By sending a specially crafted request, an attacker

could exploit this vulnerability to obtain sensitive information or cause the application to crash.
CVE-2024-37370 - MIT Kerberos 5 (aka krb5) could allow a remote attacker to bypass security restrictions, caused by improper access control. By sending a specially crafted request to modify the plaintext Extra Count field of a confidential GSS krb5 wrap token, an attacker could exploit this vulnerability to cause the unwrapped token to appear truncated to the application.
CVE-2024-6197 - cURL libcurl is vulnerable to a denial of service, caused by a memory allocation flaw in the utf8asn1str() function in the ASN1 parser. By using a specially crafted TLS certificate, a remote attacker could exploit this vulnerability to cause a denial of service condition.
CVE-2024-37371 - MIT Kerberos 5 (aka krb5) is vulnerable to a denial of service, caused by an invalid memory reads during GSS message token handling. By sending specially crafted message tokens, a remote authenticated attacker could exploit this vulnerability to cause a denial of service condition.

Affected Products and Versions

Affected Product(s)	Version(s)
PowerSC	1.3, 2.0, 2.1, 2.2

The vulnerabilities in the following filesets are being addressed:

Fileset	Lower Level	Upper Level
powerscStd.tnc_pm	1.3.0.4	2.2.0.3
curl-8.9.1-1.aix7.1.ppc.rpm	7.19.4	8.7.1
krb5-libs-1.21.3-1.aix7.1.ppc.rpm	1.18.0.0	1.21.2.1

Link

Hardware alerts:

- **HIPER: The latest service pack 1060.20 is now available for system firmware levels, ML1060, MM1060 and MH1060.**

This service pack includes the following Security/HIPER issues:
Security problems were fixed for CVE-2022-0480 and CVE-2023-6531
HIPER: A problem was fixed for a possible partition or system hang accompanied by an SRC BC10E504 error log.
Visit Fix Central for all the latest updates.
Date first published
22 November 2024
Power Firmware

HIPERIBM Power E1050 (9043-MRX)	Platform Independent All Versions
HIPERIBM Power L1022 (9786-22H)	Platform Independent All Versions
HIPERIBM Power L1024 (9786-42H)	Platform Independent All Versions
HIPERIBM Power S1014 (9105-41B)	Platform Independent All Versions
HIPERIBM Power S1022 (9105-22A)	Platform Independent All Versions
HIPERIBM Power S1022s (9105-22B)	Platform Independent All Versions

HIPERIBM Power System E1080 Server (9080-HEX)
Platform Independent All Versions
HIPERIBM Power System S1012 (9028-21B)
Platform Independent All Versions
Link and Link

IBM Spectrum Scale / ESS alerts:

- **These fixpacks are cumulative and includes all fixes completed since the last release.**
  - Storage_Scale_Data_Management-5.1.9.7-ppc64-AIX-update
  - Storage_Scale_Standard-5.1.9.7-s390x-Linux
  - Storage_Scale_Advanced-5.1.9.7-s390x-Linux
  - Storage_Scale_Standard-5.1.9.7-x86_64-Linux
  - Storage_Scale_Data_Management-5.1.9.7-ppc64LE-Linux
  - Storage_Scale_Advanced-5.1.9.7-x86_64-Linux
  - Storage_Scale_Data_Access-5.1.9.7-ppc64LE-Linux
  - Storage_Scale_Data_Access-5.1.9.7-ppc64-AIX-update
  - Storage_Scale_Standard-5.1.9.7-x86_64-Windows
  - Storage_Scale_Data_Management-5.1.9.7-s390x-Linux
  - Storage_Scale_Standard-5.1.9.7-ppc64LE-Linux
  - Storage_Scale_Advanced-5.1.9.7-ppc64LE-Linux
  - Storage_Scale_Data_Access-5.1.9.7-s390x-Linux
  - Storage_Scale_Data_Management-5.1.9.7-x86_64-Linux
  - Storage_Scale_Erasure_Code-5.1.9.7-x86_64-Linux
  - Storage_Scale_Advanced-5.1.9.7-ppc64-AIX-update
  - Storage_Scale_Data_Access-5.1.9.7-x86_64-Linux
  - Storage_Scale_Data_Access-5.1.9.7-x86_64-Windows
  - Storage_Scale_Standard-5.1.9.7-ppc64-AIX-update

- **IBM Storage Scale System has identified an issue in drive firmware that may cause a drive to be marked as failed**

  Recently, a defect was identified in some of the IBM Storage Scale System drive firmware. After a drive firmware update, a head alignment process is initiated, which can take up to 4 hours to complete. During this alignment process, the drive heads might not be perfectly aligned, potentially leading to retries, performance issues, and intervention by GNR disk hospital. In severe cases, the drive may be flagged as failed due to excessively high bit error rates, checksum errors, or insufficient overall performance. It's important to note that this process does not inherently lead to data corruption or loss.

  Users Affected

  Users upgrading to the following drive firmware levels are affected:

  SCP2, TCP2, SCP4, TCP4, SCP5, TCP5, SCP8, TCP8
  SCL2, NCL2, SCL3, NCL3, SCL4, NCL4, SCL6, NCL6

This can be hit on Storage Scale System 5000 running all currently supported code levels (Storage Scale System 6.1.0.0 through 6.1.9.4 and Storage Scale System 6.2.0.0 through 6.2.1.1).

Problem Determination

Run the following command to see if the system drives have the affected firmware:

mmlsfirmware --type drive

Recommendation

Upgrade to the latest drive firmware.

Link

- **IBM Storage Scale Software Version Recommendation**

  This generalised recommendation is made available to assist clients in implementing a code update strategy. It is a full field perspective, and as such, a customised recommendation that takes into account specifics such as business upgrade windows, length of time since last update, decommission plans. might require assistance from local support teams. In general, recommendations assume planning updates annually. Detailed information on the product fixes contained within IBM Storage Scale v5.x releases can be found here.

IBM Storage Scale	Minimum Recommended Level	Latest Level
IBM Storage Scale	5.1.9.x stream2: 5.1.9.3 [Apr 2024] 5.2.x stream: 5.2.0.0 [Apr 2024]	5.1.9.x stream2: 5.1.9.7 [Nov 2024] 5.2.x stream: 5.2.1.1 [Sep 2024]
IBM Storage Scale System (ESS)	5.1.x stream: ESS 6.1.9.2 [Mar 2024]	5.1.x stream: ESS 6.1.9.4 [Oct 2024]
IBM Storage Scale System 3000, 3200, 3500, 5000, and 6000	5.1.x stream: ESS 6.1.9.2 [Mar 2024] 5.2.x stream: ESS 6.2.0.1 [Jun 2024]	5.1.x stream: ESS 6.1.9.4 [Oct 2024] 5.2.x stream: ESS 6.2.1.1 [Oct 2024]
IBM Storage Scale Container Native Storage Access (CNSA)	5.1.9 stream: 5.1.9.7 [Nov 2024]	5.2.x stream: 5.2.1.1 [Sep 2024]
IBM Storage Scale Container Storage Interface (CSI) (stndalone)	2.10.x stream: 2.10.5 [Nov 2024]	2.11.x stream: 2.12.1 [Sep 2024]

Link

Have some time off and get ready for the next patching cycle (looks busy if the above is any indication!) All the best from Belisama for a great ‘25
Keep safe
Red, Belisama