Belisama

September Newsletter

Subscribe/Unsubscribe

Greetings all,
It was a pleasure to catch-up with so many colleagues in Vegas and, even though I felt the conference was a little overly focused on AI, there were enough Power updates there to satisfy my curiosity.

A few updates to share

- This is also the time to renew or nominate as IBM Champion. I was asked recently why I was an IBM Champion – and my answer was two reasons… Firstly there is the chance to work with the best Power experts around the world with access to the IBM development teams and secondly there is the ability to influence the direction IBM is taking on the products that I love.
  The process has also changed this year, with a range of advocacy badges that you can earn on the way to becoming a champion.
  Champion nomination
- There will be a smaller TechXchange in Sydney at the end of November, so look out for updates.
  Please let me know if there are any sessions that would be interested in attending – and I will see if I can get added to the agenda.

Quick bites

Why AIX running on Power10 is a winning combination.
In case you wondered….
Link

New SAP SD Benchmark: 1,65 Mio SAPS with Power10
SAP published today in SAP’s Benchmark Directory a new SD Benchmark (#23059) for IBM Power10 E1080 – 16 Sockets, 240 Cores, 1,65 MIO SAPS!
Link
Certification

AIX SUMA and PowerVS - "0500-059 Entitlement is required to download. The system's serial number is not entitled"
A number of customers using SUMA in PowerVS have reported suddenly getting entitlement errors, even thought all servers in PowerVS are automatically entitled. It was found that their country code details were wrong – so the fix is to check the contents of `/var/suma/data/config.suma` and fix.

Introducing the integration of IBM Power Virtual Server with IBM Key Protect for AIX and Linux

The transfer of data and procedures from legacy systems to the cloud necessitates adherence to current data security protocols and regulations for handling data at rest, data in transit and data in use. It comes as no surprise that organisations have identified security and data protection as the primary obstacles when it comes to migrating sensitive applications and data to the public cloud. Despite the advantages of cloud-ready architectures, such as simplicity and support for micro-services, concerns persist regarding the potential mishandling of data by the cloud service provider. Organisations want to encrypt their data in the cloud using their own encryption keys and retain control over and manage these keys.

Link

HMC Scanner for POWER Server Config and Performance Stats

Use the HMC Scanner to quickly extract all the details of the POWER Servers the HMC is connected too and saved in a Microsoft Excel spreadsheet.

The latest version is 0.11.50.

Link

In case you missed ….

- **ASEANZK Power meetup**

  In case you missed the September ASEANZK Power meetup, which introduced the IBM Cloud Management Console for Power Systems, I have uploaded the recording and slides to the IBM Community page. Thanks to Hari and Manju for a great overview of CMC and the demonstration of the key features.

  Link
- **Latest Power VUG**

  I was lucky to be able to attend the latest VUG (Panel discussion) in person, the recording should be available soon from their site.

  Link
- **TechXchange**

  If you missed the TechXchange, some of the main sessions and offers are now available on demand.

  Link
- **PowerVM VIO Server**

  Preparing customer firewalls and proxies for the upcoming infrastructure changes – Call Home, Electronic Fix Distribution

  New network connections between your machine and IBM servers are required to keep your ability to perform Call Home and download fixes. If you have a firewall in your network, you might need to make changes to allow the new connections.

  Note 1: IP addresses are subject to change. Use DNS names whenever possible.

  Note 2: Applies to protocols HTTPS (port 443)

  Link

Redbooks and Redpapers

- **SAP HANA on IBM Power Systems Architectural Summary** , Draft Redpaper, 22 September 2023
  Link

IBM alerts and notices

AIX HIPER:

- **APAR IJ47907: Potential undetected data loss by using zlibNX**
  The zlibNX library using hardware acceleration compression on Power9/Power10 can generate incorrect compressed files that can't be uncompressed, resulting in potential undetected data loss if the original uncompressed data is no longer available. At the time of compression, there is a rare error path that will generate incorrect compressed data with no error or warning reported, and the resulting file cannot be uncompressed. This issue has been seen with DB2 compression and standard compress tools such as pigz, but can be seen with any application that uses zlibNX.

  Recommended Action

  Affected AIX Levels and Recommended Fixes *

Min Affected Level	Max Affected Level	Fixing Level
AIX 7300-01-00 zlibNX.rte 7.3.1.0	AIX 7300-01-02-2320 zlibNX.rte 7.3.1.1	AIX 7300-01-03
AIX 7300-00-00 zlibNX.rte 7.3.0.0	AIX 7300-00-04-2320 zlibNX.rte 7.3.0.3	AIX 7300-00-05
AIX 7200-05-00 zlibNX.rte 7.2.4.0	AIX 7200-05-06-2320 zlibNX.rte 7.2.4.9	AIX 7200-05-07

  *For applicable levels, the HIPER ifixes in this column include the zlibNX security vulnerability fixes from:
  https://aix.software.ibm.com/aix/efixes/security/zlib_advisory2.asc

  This table describes which active levels are affected and where to obtain fixes. Before the APAR fix is available, an interim fix (iFix) is available for each affected level.
  The available interim fixes might apply only to the latest Service Packs. If a custom interim fix is required, contact IBM Support. The interim fixes can be downloaded from the same location by using HTTPS or FTPS.
  Link

AIX alerts:

- **Drives shipped on select IBM Power Systems may contain a potential security vulnerability.**

  A limited number of IBM Power Systems drives were inadvertently shipped with an IBM internal test image present on the disk. This test image (AIX) is not intended for use outside IBM and is not shipped in a secure state for external use. IBM has developed a mitigation plan for users who may inadvertently be running these images. If you have implemented your own fresh install of AIX or restored your own distribution of AIX, you are not exposed. IBM recommends you verify your instance(s) of AIX are not exposed by reviewing this notice and performing the recommended verification and remediation.

  Recommended Action

  IBM strongly recommends addressing the potential vulnerability now.
  To determine if your current AIX contains the exposure, a system administrator should run the following AIX command:

  ```
  lslpp -l htx
  ```

  if HTX is NOT found (no exposure) the command output should contain “htx not installed” as in the example below:

  ```
  lslpp: 0504-132 Fileset htx not installed.
  ```

  If the system is exposed, the command output will contain “COMMITTED Hardware Test Executive” as seen in the example below:

  ```
  Fileset Level State Description
  -------------------------------------------------------
  Path: /usr/lib/objrepos
  htx 7.3.1.166 COMMITTED Hardware Test Executive
  ```

  To remove HTX issue the following command:

  ```
  installp -u htx
  ```

  Monitor for the following confirmation for the output to indicate “DEINSTALL SUCCESS” as shown in the following example output:

  ```
  htx      7.3.1.170     USR        DEINSTALL   SUCCESS
  ```

  After the removal of the lpp, a reboot of the OS is needed to complete the removal, however the exposure has been mitigated and the OS reboot can be scheduled later.

  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-2022-40609 - IBM SDK, Java Technology Edition 7.1.5.18 and 8.0.8.0 could allow a remote attacker to execute arbitrary code on the system, caused by an unsafe deserialization flaw. By sending specially-crafted data, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 236069.

CVE-202 -

DESCRIPTION: An unspecified vulnerability in Java SE related to the Libraries component could allow a remote attacker to cause low integrity impacts.

Affected Products and Versions

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

Link

- **AIX is vulnerable to denial of service due to ISC BIND (CVE-2023-2828).**

A vulnerability in ISC BIND could allow a remote attacker to cause a denial of service (CVE-2023-2828). AIX uses ISC BIND as part of its DNS functions.

Vulnerability Details

CVE-2023-2828 - ISC BIND is vulnerable to a denial of service, caused by a flaw that allows the named's configured cache size limit to be significantly exceeded. By querying the resolver for specific RRsets in a certain order, a remote attacker could exploit this vulnerability to exhaust all memory on the host.

Affected Products and Versions

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

The following fileset levels are vulnerable:

Fileset	Lower Level	Upper Level
bind.rte	7.1.916.0	7.1.916.2602

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-2022-40609 - IBM SDK, Java Technology Edition 7.1.5.18 and 8.0.8.0 could allow a remote attacker to execute arbitrary code on the system, caused by an unsafe deserialization flaw. By sending specially-crafted data, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 236069.

CVE-2023-22049 - An unspecified vulnerability in Java SE related to the Libraries component could allow a remote attacker to cause low integrity impacts.

Affected Products and Versions

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

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

For Java8: Less than 8.0.0.810

Link

- **Multiple vulnerabilities in OpenSSL affect AIX**

  There are multiple vulnerabilities in OpenSSL as used by AIX. OpenSSL is used by AIX as part of AIX's secure network communications.

  Vulnerability Details

  CVE-2023-0464 - OpenSSL is vulnerable to a denial of service, caused by an error related to the verification of X.509 certificate chains that include policy constraints. By creating a specially crafted certificate chain that triggers exponential use of computational resources, a remote attacker could exploit this vulnerability to cause a denial of service.

  CVE-2023-2650 - OpenSSL is vulnerable to a denial of service, caused by a flaw when using OBJ_obj2txt() directly, or use any of the OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no message size limit. By sending a specially crafted request, a remote attacker could exploit this vulnerability to cause a denial of service.

  CVE-2023-0465 - OpenSSL could allow a remote attacker to bypass security restrictions, caused by a flaw when using a non-default option to verify certificates. By using invalid certificate policies in leaf certificates, an attacker could exploit this vulnerability to bypass policy checking.

  CVE-2023-0466 - OpenSSL could allow a remote attacker to bypass security restrictions, caused by a flaw in the X509_VERIFY_PARAM_add0_policy function. By using invalid certificate policies, an attacker could exploit this vulnerability to bypass certificate verification.

  CVE-2023-2975 - OpenSSL could allow a remote attacker to bypass security restrictions, caused by AES-SIV cipher implementation. By sending a specially-crafted request using empty data entries as associated data, an attacker could exploit this vulnerability to bypass authentication validation.

  CVE-2023-3446 - OpenSSL is vulnerable to a denial of service, caused by a flaw when using the DH_check(), DH_check_ex() or EVP_PKEY_param_check() functions to check a DH key or DH parameters. By sending a specially crafted request using long DH keys or parameters, a remote attacker could exploit this vulnerability to cause long delays, and results in a denial of service condition.

  CVE-2023-3817 - OpenSSL is vulnerable to a denial of service, caused by a flaw when using the DH_check(), DH_check_ex() or EVP_PKEY_param_check() functions to check a DH key or DH parameters.

By sending a specially crafted request, a remote attacker could exploit this vulnerability to cause long delays, and results in a denial of service condition.

Affected Products and Versions

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

Link

AIX APARs:

- **APARs (Authorised Program Analysis Reports):**
  - IJ48574: INSECURE PERMISSIONS – SMBC
    Root owned directories /var/adm/smbc and /var/adm/smbc/smbcgssd_krb5cc have world writable permissions.
  - IJ48617: UNIX SOCKET LOCK PAIR PROBLEMS IN SOFREE2
    The user may see a callstack similar to the following: pvthread+088C00 STACK:
  - IJ48607: LIVE UPDATE PREVIEW FAILS WITH SSP
    Live update fails using shared storage pools
  - IJ48582: LIVE UPDATE PREVIEW FAILS WITH SSP
    Live update fails using shared storage pools
  - IJ48599: READVGDA PREFERRED READ VALUE FOR SVG W/ MIRROR POOLS INCORRECT
    For scalable VGs that use mirror pools, the preferred read
  - IJ48648: BOS.ESAGENT UPGRADE MAY FAIL IF IBM.ESAGENT WAS ACTIVATED
    The upgrade of the fileset bos.esagent may fail if the IBM.ESAGENT is actived.
  - IJ48641: A POTENTIAL SECURITY ISSUE EXISTS
    This APAR addresses a potential security issue.
  - IJ48589: LPAR CRASHED @TCP_TRACE+00009C
    System may crash when tcp_ndebug network option is set to 0. With following stack trace:
  - IJ48581: THERE IS NO WAY TO ENABLE/DISABLE TLSV1.3
    There is no way to enable/disable TLSv1.3
  - IJ48638: ECHO WRITES ADDITIONAL NEW LINE
    echo writes additional new line
  - IJ48597: UPDATE PACKDEP.MK FOR DEFECT 1172043
    Dependencies updated for defect 1172043
  - IJ48656: IBV_CREATE_AH() WILL FAIL FOR ROCEV2 MODE
    ibv_create_ah() will fail in RoCEv2 mode when called.
  - IJ48592: PASSWORD CHANGE ATTEMPT FAILS
    A password change attempt may fail - returning you to the command prompt - after only prompting for the new password.

- IJ48658: UPDATE LIBODM TO USE 64 BIT LIBVIOCMNOTIFY.A
  When some commands run from HMC on VIOS through viosvrcmd, there may be inconsistent state between VIOS, and HMC
- IJ48616: LIVE UPDATE PREVIEW FAILS WITH SSP
  Live update fails using shared storage pools
- IJ48642: VIOS UPGRADE MAY HANG IN CLUSTER ENVIRONMENT.
  VIOS upgrade may hang in cluster environment
- IJ48622: READVGDA PREFERRED READ VALUE FOR SVG W/ MIRROR POOLS INCORRECT
  For scalable VGs that use mirror pools, the preferred read
- IJ48608: A POTENTIAL SECURITY ISSUE EXISTS
  This APAR addresses a potential security issue.
- IJ48618: A POTENTIAL SECURITY ISSUE EXISTS
  This APAR addresses a potential security issue.
- IJ48649: LPAR CRASHED @TCP_TRACE+00009C
  System may crash when tcp_ndebug network option is set to 0. With following stack trace:
- IJ48583: UPDATE PACKDEP.MK FOR DEFECT 1172043
  Update for defect 1172043
- IJ48635: CONSOLE SPAMMING SUCCESSFULLY UPDATED THE KERNEL
  Throughout install & update, the console output is full of unhelpfull messages
- IJ48591: READVGDA PREFERRED READ VALUE FOR SVG W/ MIRROR POOLS INCORRECT
  For scalable VGs that use mirror pools, the preferred read
- IJ48595: THERE IS NO WAY TO ENABLE/DISABLE TLSV1.3
  There is no way to enable/disable TLSv1.3
- IJ48606: LPAR CRASHED @TCP_TRACE+00009C
  System may crash when tcp_ndebug network option is set to 0. With following stack trace:
- IJ48601: SSH PUBLIC KEY AUTHENTICATION FAILS IF NO PASSWORD DEFINED
  If a user is created without a password, for the purpose of public key authentication only, login will fail
- IJ48588: PACKAGING CHANGES NEEDED FOR MIGRATION FOR OFED.CONF
  Packaging changes needed for migration for ofed.conf
- IJ48613: LPAR CRASHED @TCP_TRACE+00009C
  System may crash when tcp_ndebug network option is set to 0. With following stack trace:
- IJ48596: LIVE UPDATE PREVIEW FAILS WITH SSP
  Live update fails using shared storage pools
- IJ48600: SSHD MAY CORRUPT SYSENVIRON AND AFFECT AT JOBS
  In some circumstances, it is possible for sshd to corrupt SYSENVIRON.

- IJ48602: A POTENTIAL SECURITY ISSUE EXISTS
  This APAR addresses a potential security issue.
- IJ48612: LPAR CRASHED @ NFS4_PUT_RESARRAY
  System crash at nfs4_put_resarray().
- IJ48637: ECHO WRITES ADDITIONAL NEW LINE
  echo writes additional new line
- IJ48580: LPAR CRASHED @ NFS4_PUT_RESARRAY
  System crash at nfs4_put_resarray().
- IJ48594: LPAR CRASHED @ NFS4_PUT_RESARRAY
  System crash at nfs4_put_resarray().
- IJ48619: SYSTEM CALL INPUT VALIDATION – NETINFO
  The user may see a callstack similar to the following: pvthread+10C700 STACK:
- IJ48636: OD -T FAILS WITH EXIT CODE ZERO
  'od -t' doesnt output usage error.
- IJ48604: EXTRA BREAK STATEMENT IN THE MIDDLEWARE FIND_DEVICES CODE PATH
  no retry if valvfc_validate_luns() failed
- IJ48657: A POTENTIAL SECURITY ISSUE EXISTS
  This APAR addresses a potential security issue.
- IJ48671: A POTENTIAL SECURITY ISSUE EXISTS
  This APAR addresses a potential security issue.
- IJ48651: TRUSTCHK FAILURE FOR FILE /USR/LIB/LIBLPMCOMMON.A
  Trustchk reports error for /usr/lib/liblpmcommon.a for it's size attribute verification failure.
- IJ48667: VIOS CAN CRASH DURING ASYNC EVENT ON UNMAPPED VFCHOST
  After unmapping vfchost, a crash may occur on the VIOS when trying to forward and asynchronous event to client
- IJ48666: A POTENTIAL SECURITY ISSUE EXISTS
  This APAR addresses a potential security issue.
- IJ48663: A POTENTIAL SECURITY ISSUE EXISTS
  This APAR addresses a potential security issue.

PowerSC alerts:

- **Multiple vulnerabilities in Curl affect PowerSC**
  There are multiple vulnerabilities in Curl that affect PowerSC.
  Vulnerability Details
  - CVE-2023-28320 - cURL libcurl is vulnerable to a denial of service, caused by a race condition flaw in the siglongjmp() function. By sending a specially crafted request, a remote attacker could exploit this vulnerability to cause the application to crash or misbehave.
    CVE-2023-28322 - cURL libcurl could allow a remote attacker to bypass security restrictions, caused by a flaw in the logic for a reused handle when it is (expected to be) changed from a PUT to a POST.. By sending a specially

crafted request, an attacker could exploit this vulnerability to cause application to misbehave and either send off the wrong data or use memory after free or similar in the second transfer.

CVE-2023-28319 - cURL libcurl could allow a remote attacker to obtain sensitive information, caused by a use-after-free flaw in SSH sha256 fingerprint check. By sending a specially crafted request, an attacker could exploit this vulnerability to obtain sensitive heap-based data from the error message, and use this information to launch further attacks against the affected system.

CVE-2023-28321 - cURL libcurl could allow a remote attacker to bypass security restrictions, caused by a flaw when listed as "Subject Alternative Name" in TLS server certificates. By sending a specially crafted request, an attacker could exploit this vulnerability to accept mismatch wildcard patterns.

Affected Products and Versions

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

Link

ESS Technote:

- **IBM Elastic Storage System 3500 out of memory condition**

  ESS 5000 systems using MOFED 5.9-0.5.6.1 with Mellanox cards can potentially see an out of memory condition. The issue can be seen faster with Ethernet cards with MTU 9000 and tx and rx ring size set to the maximum size of 8192 with heavy TCP traffic.

  To know if your system is exposed to this issue, you can run the following commands:

```
# ofed_info -s
MLNX_OFED_LINUX- 5.9-0.5.6.1:

# ethtool -g enP51p1s0f0
Ring parameters for enP51p1s0f0:
Pre-set maximums:
RX:             8192
RX Mini:        n/a
RX Jumbo:       n/a
TX:             8192
Current hardware settings:
RX:             8192
RX Mini:        n/a
RX Jumbo:       n/a
TX:             8192
```

  Link

Keep safe and talk soon,
Red, Belisama