Belisama

May Newsletter

Subscribe/Unsubscribe

Greetings all,
Trust you are all keeping safe and well? Just a short update this month as we have been busy assisting customers with migrations, finalising a GLVM tips document (hope to publish soon) and getting ready for Techfest and then TechXchange in Vegas later this year (hope to see you there!).

Quick bites

Ansible power_aix collection (release 1.6.1) is now available
A few handy new additions:

- New module: Bosboot.
- New Playbooks: mktun, mount,installp, user, mpio, mkfilt,
- New Playbooks: bosboot, group, tunables, filesystem, nim_suma, logical_volume
- New Playbooks: tunfile_mgmt, mktcpip, inittab
- Enhanced idempotency for devices module.
- Enhancement in nim_alt_disk_migration:
- Target disk without PVID accepted

… and many more, including some much needed fixes – see Link

In case you missed ….

- **AIX Support Trends and updateS**
  The May Power VUG session featured trends and updates for IBM Power Systems led by Rama Tenjarla and AIX Development/Support.
  Topics covered include LDAP, Kerberos, PAM, PowerVC, SMBC, DNF for open source software, and IO performance.
  For slides and the recording, see Link
- **ASEANZK AIX/IBM i/Linux on Power Meetup Group**
  The last meetup held on 12th May looked at antivirus protection for IBM i, AIX and Linux.
  Summary:

  > No OS can afford to be unprotected. IBM i, IBM AIX and Linux on Power systems are typically known for running critical workloads and applications. This means the threat of viruses, malware, and ransomware pose a significant risk to your organisation. This Meetup will cover Powertech Antivirus that is designed to provide the level of protection your Power Systems servers need.

  This session was presented by Rohit Mathur and the recording / slides can be downloaded from:
  Meetup
  IBM Community

Coming soon

- **IBM TechXchange 11-14 September 2023 (Las Vegas)**
  The IBM TechXchange 11-14 September 2023 (Las Vegas) is an event that brings together industry experts, thought leaders, clients & partners to discuss and share knowledge on the latest technology from IBM. This year's event will have a track dedicated to cybersecurity, with a particular emphasis on:
    - Threat management (QRadar SIEM, ReaQta & QRadar SOAR)
    - Data security (Guardium)
    - Identity & access management (Verify)
    - Mobile Security management (MaaS360)
    - Advanced Fraud Protection (Trusteer)

  I don’t see much focus on Power and infrastructure – so I hope that you will also be submitting papers (by 5th June)!
  Link
- **IBM TechFest 5th June**
  TechFest is the only deep technical event available to the entirety of Technology Expert Labs, Customer Success, and IBM TEL Partners.
  It brings our technical ecosystems together to share expertise and knowledge, providing deep technical hands on experience with our software which helps drive innovation and business value for our clients.
  Link

Redbooks and Redpapers

- **IBM Power Systems Virtual Server Guide for IBM AIX and Linux**, Redpaper, revised: 19 May 2023
  Link
- **SAP HANA on IBM Power Systems Virtual Servers: Hybrid Cloud Solution**, Redbook, published: 29 April 2023, updated 03 May 2023
  Link

IBM alerts and notices

Power firmware alerts:

- **PowerVM vulnerable to an undetected violation of the LPAR isolation (CVE-2023-30438)**
  An internally discovered vulnerability in PowerVM on IBM Power9 and Power10 systems could allow an attacker with privileged user access to a logical partition to perform an undetected violation of the isolation between logical partitions which could lead to data leakage or the execution of arbitrary code in other logical partitions on the same physical server.
  There are a number of good blogs and bulletins:
    - PSIRT Blog
    - CVE Security Bulletin

Vulnerability Details

CVEID: CVE-2023-30438

DESCRIPTION: A vulnerability was identified in IBM PowerVM that could lead to an undetected violation of the isolation between partitions.

Affected Products and Versions

Affected Product(s)	Version(s)
PowerVM Hypervisor	FW1030.00 - FW1030.10
PowerVM Hypervisor	FW1020.00 - FW1020.30
PowerVM Hypervisor	FW1010.00 - FW1010.50
PowerVM Hypervisor	FW950.00 - FW950.70

Remediation/Fixes

- IBM strongly recommends customers with the Power9 below install FW950.71(950_124) or newer to remediate this vulnerability.

Power 9

1. IBM Power System L922 (9008-22L)
2. IBM Power System S922 (9009-22A, 9009-22G)
3. IBM Power System H922 (9223-22H, 9223-22S)
4. IBM Power System S914 (9009-41A, 9009-41G)
5. IBM Power System S924 (9009-42A, 9009-42G)
6. IBM Power System H924 (9223-42H, 9223-42S)
7. IBM Power System E950 (9040-MR9)
8. IBM Power System E980 (9080-M9S)

- IBM strongly recommends customers with the Power10 below install: FW1010.51(1010_163), FW1030.11(1030_052) or newer to remediate this vulnerability.

Power 10

1. IBM Power System E1080 (9080-HEX)

- IBM strongly recommends customers with the Power10 below install: FW1020.31(1020_102), FW1030.11(1030_058) or newer to remediate this vulnerability.

Power 10

1. IBM Power System S1022 (9105-22A)
2. IBM Power System S1024 (9105-42A)
3. IBM Power System S1022s (9105-22B)
4. IBM Power System S1014 (9105-41B)
5. IBM Power System L1022 (9786-22H)
6. IBM Power System L1024 (9786-42H)
7. IBM Power System E1050 (9043-MRX)

Link

- **AIX is vulnerable to arbitrary code execution due to libxml2 (CVE-2022-40303 and CVE-2022-40304)**

  UPDATED May 4:

  Corrected the affected upper fileset levels for AIX 7.2 TL5 to show that SP06 is affected. Corrected the affected upper fileset levels for AIX 7.3 TL1 to show that SP02 is affected. Corrected the affected upper fileset levels for VIOS to show that VIOS 3.1.4.21 is affected. Added iFixes for AIX 7.2 TL5 SP06 and 7.3 TL1 SP02. Added iFix for VIOS 3.1.4.21.

  Vulnerabilities in libxml2 could allow a remote attacker to execute arbitrary code (CVE-2022-40303 and CVE-2022-40304). AIX uses libxml2 as part of its XML parsing functions.

  Vulnerability Details

  CVE-2022-40304: Gnome ibxml2 could allow a remote attacker to execute arbitrary code on the system, caused by a dict corruption flaw. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system.

  CVE-2022-40303: Gnome libxml2 could allow a remote attacker to execute arbitrary code on the system, caused by an integer overflow in the XML_PARSE_HUGE function. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system.

  Affected Products and Versions

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

  Link

- **AIX is vulnerable to security restrictions bypass due to curl (CVE-2022-32221)**

  Vulnerability in cURL libcurl could allow a remote attacker to bypass security restriction (CVE-2022-32221). AIX uses cURL libcurl as part of LV/PV encryption integration with HPCS.

Vulnerability Details

CVE-2022-32221: cURL libcurl could allow a remote attacker to bypass security restrictions, caused by a flaw when using the read callback (CURLOPT_READFUNCTION) to ask for data to send. By sending a specially-crafted request, an attacker could exploit this vulnerability to send wrong data or doing a use-after-free is not present in libcurl code.

Affected Products and Versions

Affected Product(s)	Version(s)
AIX	7.3 TL1

The following fileset levels are vulnerable:

Fileset	Lower Level	Upper Level
oss.lib.libcurl	7.79.1.0	7.79.1.0

Link

- **Multiple vulnerabilities in IBM Java SDK affect AIX**

Vulnerability Details

CVE-2022-21426: An unspecified vulnerability in Java SE related to the JAXP component could allow an unauthenticated attacker to cause a denial of service resulting in a low availability impact using unknown attack vectors.
CVE-2023-21830: An unspecified vulnerability in Java SE related to the Serialisation component could allow a remote attacker to cause a denial of service resulting in a low integrity impact using unknown attack vectors.
CVE-2023-21843: An unspecified vulnerability in Java SE related to the Sound component could allow a remote attacker to cause a denial of service resulting in a low integrity impact using unknown attack vectors.
CVE-2023-30441: IBM Runtime Environment, Java Technology Edition IBMJCEPlus and JSSE 8.0.7.0 through 8.0.7.11 components could expose sensitive information using a combination of flaws and configurations. IBM X-Force ID: 253188.

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 8.0.0.800

Note: To find out whether the affected Java filesets are installed on your systems, refer to the lslpp command found in AIX user's guide.

Example: lslpp -L | grep -i java

Link

- **AIX is vulnerable to HTTP request smuggling due to Perl (CVE-2022-31081)**

A vulnerability in libwww-perl could allow an attacker to poison web caches, bypass web application firewall protection, and conduct XSS attacks (CVE-2022-31081). AIX uses Perl in various operating system components.

Vulnerability Details

CVE-2022-31081: Libwww is vulnerable to HTTP request smuggling, caused by an unspecified flaw. By sending a specially-crafted HTTP(S) transfer-encoding request header, an attacker could exploit this vulnerability to poison the web cache, bypass web application firewall protection, and conduct XSS attacks.

Affected Products and Versions

Affected Product(s)	Version(s)
AIX	7.1
AIX	7.2
AIX	7.3
VIOS	3.1

Link

AIX and PowerVM notifications:

- **Preparing customer firewalls and proxies for the upcoming infrastructure changes – Call Home, Electronic Fix Distribution**
  Public internet IP addresses are changing for the IBM servers that support Call Home and electronic download of fixes for customer system's software, hardware, and operating system. This change pertains to all operating systems and applications connecting to IBM for electronic Call Home and fix download.
  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.
  Link

PowerHA notifications:

- **PowerHA fix information for PowerHA 7.2.4 Service Pack 7**
  PowerHA 7.2.4 Service Pack 7 is now available for download as of April 2023.
  NOTE: PowerHA SystemMirror 7.2.4 SP7 testing has been done on the following AIX levels and are recommended:
  - AIX7.3 TL01 SP1*
  - AIX7.3 TL00 SP3
  - AIX7.2 TL05 SP5
  - AIX7.2 TL04 SP6
  - AIX7.2 TL03 SP7
  - AIX7.2 TL02 SP6
  - AIX7.2 TL01 SP6
  - AIX7.1 TL05 SP10

  *Note: AIX7.3 TL01 SP1 requires a critical AIX APAR IJ44756 for PowerHA GUI Cluster discovery to work.
  Link

GPFS/Spectrum Scale notifications:

- **IBM Spectrum Scale Webinar – Installer Toolkit (20th June 22:00 SGT, 00:00 Au)**
  Register to join the IBM Spectrum Scale Support team for a free-of-charge IBM Spectrum Scale Webinar that will discuss Installer Toolkit in IBM Spectrum Scale. IBM Spectrum Scale Webinars are hosted by IBM Spectrum Scale Support to share expertise and knowledge of the Spectrum Scale product, as well as product updates and best practices. This webinar focuses on the Installer Toolkit for IBM Spectrum Scale. See the agenda for more details. Note that our webinars are free-of-charge and held via Webex.
  Agenda
  - Purpose/Why would I want to use the installation toolkit?
  - Supported Features/Limitations

- Prerequisites
- Where can I get it?
- Where to start?
- Toolkit Phases
- Example Videos
- Trouble Shooting/Logs/Known issues
- Q&A

Register
Link

- **IBM Spectrum Scale Software Version Recommendation Preventive Service Planning**
  IBM Spectrum Scale Software Version Recommendation
  Link

Keep safe and be in touch soon,
Red, Belisama