February Newsletter

Subscribe/Unsubscribe

Greetings all,
I hope that your year (rabbit and/or ‘23) is off to a good start and you have not been caught out with the changes that IBM has been making to back end for support and dial home? (See last month’s edition).

A few updates to share

- I am really pleased to see that our hard work has paid off, and the first of our Redpapers has been published. Thank you Dino and Tim for your hard work in turning our draft it into something worthy of publication.
  IBM PowerHA SystemMirror and IBM VM Recovery Manager Solutions Updates has been brought to you by: Dino Quintero, Felipe Bessa, Shawn Bodily, Carlos Jorge Cabanas Aguero, Vera Cruz, Sachin P. Deshmukh, Dishant Doriwala, Alexander Ducut, Karim El Barkouky, Ash Giddings, Santhosh S Joshi, Youssef Largou, Jean-Manuel Lenez, Juan Prada Diez, Vivek Shukla, Kulwinder Singh, Yadong Yang and Tim Simon.
  This updates provides an overview of the current business continuity solutions for applications running on IBM Power Systems. We hope that you find it useful, and please keep an eye out, as there will be two more publications soon (Thanks to Dino and Tim!).
  Link
- I have finished a couple of update presentations / demonstrations of PowerVS HA/DR focusing on GLVM and an update on PowerSC – looking at AIX security and compliance management, auditing, AIX MFA and easy management of allow/deny lists. Please contact us if you are interested in looking into these IBM offerings in greater detail.

Quick bites

AIX Strategy Paper and Roadmap
If you are concerned about the future of AIX – check out this paper from IBM outlining it’s strategy for AIX on IBM Power to 2039 – an environment to modernise your workloads with a secure, scalable and a robust open standards based Unix OS for many years to come.
Link

IBM AIX Community badge programme
The AIX community badge program recognises AIX users who contribute regularly to the success and vitality of the community and everyone within it.
Link

AIX running on IBM Power10 is a winning combination for your business
A handy summary from IBM looking at the advantages of AIX and Power10 together – indeed a formidable combination.
Link

In case you missed ….

- **IBM Electronic Fix Distribution / IBM Fix Central systems will end support for unencrypted fix downloads**
  This is the last reminder that IBM Electronic Fix Distribution (EFD) / IBM Electronic Customer Care (ECC) / IBM Fix Central systems will stop supporting unencrypted fix downloads on February 15, 2023.
  Action might be required to ensure uninterrupted downloads.
  Link
- **Java upload utility for AIX and Linux**
  This utility helps customers transfer support data to IBM faster, securely, and more conveniently. It is a command-line client that runs on many operating system platforms (AIX, Linux, IBM i, z/OS and windows) and includes:
  - Parallel HTTPS upload (up to 15 parallel sessions are possible);
  - IBM Support File Transfer ID authentication;
  - Proxy support; and
  - File names must use standard ASCII characters (no double byte characters).

  Note that the current version does not use log4j!
  Link

- **AIX AUDIT: Enabling full path file names**
  IBM Support has published a Technote advising on how to report the full path of a file in an audit trail or audit stream. This feature was introduced in AIX 530011 and 6100-04.
  From the audit man page:

  > on [panic | fullpath]
  > Restarts the auditing system after a suspension, if the system is properly configured (for example, if the audit start command was used initially and the configuration is still valid). If auditing has already started when the command is given, only bin data collection can be changed.
  > If you specify the fullpath option, the FILE_Open, FILE_Read and FILE_Write auditing events capture the full path name of a file.
  > The "fullpath" argument is only an option to the "audit on" command, so to start auditing and enable full path names you will need to run these commands:

  ```
  # audit start
  # audit off
  # audit on fullpath
  ```

  Link

Coming soon

- **IBM TechXchange Conference 2023**
  A new global event series specifically about technology and specifically designed for experts like you to go in deep with the subject mater experts from around the world.
  - Grow your skills, increase your badge tally, engage with experts, and perhaps have an impact on IBM's roadmap.
  - Advance your technical expertise through open access to the world of IBM technology?

  Join us in Las Vegas from 11 to 14 September 2023.
  The call for Speakers will be coming soon...
  Link

- **ASEANZK AIX/IBM i/Linux on Power Meetup Group**
  The next meeting will be held on Friday 10th March at 11:30 SGT / 14:30 AEDT
  Simon Hutchinson will explain how building SQL Views should become a part of your development strategy and give examples of the common ways he builds and uses Views to make his own and that of his team easier and simpler. Why do the hard work yourself when something else can do it for you?
  Simon Hutchinson fondly known as Mr. RPG in IBM i circles, is the owner and author of RPGPGM.com, an expert in RPG, SQL, Db2 of i, an IBM i community advocate, as well as a three-time IBM Champion.
  Link

Redbooks and Redpapers

- **SAP HANA on IBM Power Systems Virtual Servers: Hybrid Cloud Solution**, Redpaper, Last updated on 01 February 2023
  Link
- **Security Implementation with Red Hat OpenShift on IBM Power Systems,** draft Redpaper publication, last updated on 08 February 2023
  Link

- **Security Implementation with Red Hat OpenShift on IBM Power Systems**, draft Redpaper publication, last updated on 08 February 2023
  Link

- **IBM PowerHA SystemMirror and IBM VM Recovery Manager Solutions Updates**, draft redpaper publication, last updated on 23 February 2023
  Link

- I**mplementation Guide for IBM ESS 3500**, draft Redbooks publication, last updated on 18 February 2023
  Link

IBM alerts and notices

AIX alerts:

- **High Impact / Highly Pervasive IJ44513/IJ44047**
  Possible system crashes processing network traffic
  IBM has seen multiple issues processing normal network traffic on recent code levels. Several timing-related issues can occur, including but not limited to:
  System crashes when routes expire due to dynamic routing
  - Memory leaks or crashes when the cached_routes feature is enabled on AIX. (# no -o cached_routes)
  - System crashes due to synchronization issues between threads referencing the route entry in TCP/IP code

  For the specific AIX (7.1,7.2 &7.3) / VIOS (3.1) levels affected, see Link

- **AIX is vulnerable to denial of service vulnerabilities**
  UPDATED Feb 10 (Added pfcdd iFix for AIX 7.2 TL5 SP5 and VIOS 3.1.4.10)
  Vulnerabilities in the AIX kernel and kernel extensions could allow a non-privileged local user to cause a denial of service (CVE-2022-43380, CVE-2022-40233, CVE-2022-39165, CVE-2022-43848, CVE-2022-43849, CVE-2022-39164).
  Details

  CVEID: CVE-2022-43380 - IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX NFS kernel extension to cause a denial of service. IBM X-Force ID: 238640.
  CVEID: CVE-2022-40233 - IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX TCP/IP kernel extension to cause a denial of service. IBM X-Force ID: 235599.
  CVEID: CVE-2022-39165 - IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in CAA to cause a denial of service. IBM X-Force ID: 235183.
  CVEID: CVE-2022-43848 - IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX perfstat kernel extension to cause a denial of service. IBM X-Force ID: 239169.
  CVEID: CVE-2022-43849 - IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in the AIX pfcdd kernel extension to cause a denial of service. IBM X-Force ID: 239170.
  CVEID: CVE-2022-39164 - IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in the AIX kernel to cause a denial of service. IBM X-Force ID: 235181.

  Affected Products and Versions

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

Link

- **AIX is vulnerable to arbitrary code execution due to libxml2**

  Vulnerabilities in libxml2 could allow a remote attacker to execute arbitrary code. AIX uses libxml2 as part of its XML parsing functions.

  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 Product(s)	Version(s)
AIX	7.2
AIX	7.3
VIOS 3	.1

  Link

PowerSC alerts:

- **PowerSC is vulnerable to information disclosure due to Bouncy Castle (CVE-2020-15522)**

  A vulnerability in Bouncy Castle could allow a remote attacker to obtain sensitive information, which could be exploited to obtain private key information (CVE-2020-15522). PowerSC uses Bouncy Castle for cryptography.

  Details

  CVEID: CVE-2020-15522 - Bouncy Castle BC Java, BC C# .NET, BC-FJA, BC-FNA could allow a remote attacker to obtain sensitive information, caused by a timing issue within the EC maths library. By utilise cryptographic attack techniques, an attacker could exploit this vulnerability to obtain the private key information, and use this information to launch further attacks against the affected system.

  Affected Products and Versions

Affected Product(s)	Version(s)
PowerSC	All

  Link

- **Multiple vulnerabilities in Curl affect PowerSC**

  The following vulnerabilities in cURL have been identified:

  Details

CVEID: CVE-2022-32206 - cURL libcurl is vulnerable to a denial of service, caused by a flaw in the number of acceptable "links" in the "chained" HTTP compression algorithms. By persuading a victim to connect a specially-crafted server, a remote attacker could exploit this vulnerability to insert a virtually unlimited number of compression steps, and results in a denial of service condition.

CVEID: CVE-2022-32207 - cURL libcurl could allow a remote attacker to obtain sensitive information, caused by improper preservation of permissions when saving cookies, alt-svc and hsts data to local files. By sending a specially-crafted request, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.

CVEID: CVE-2022-32208 - cURL libcurl is vulnerable to a man-in-the-middle attack, caused by a flaw in the handling of message verification failures. An attacker could exploit this vulnerability to launch a man-in-the-middle attack and gain access to the communication channel between endpoints to inject data to the client..

CVEID: CVE-2022-32205 - cURL libcurl is vulnerable to a denial of service, caused by an issue with the ability to set excessive amounts of Set-Cookie: headers in a HTTP response to curl by a server. By persuading a victim to connect a specially-crafted server, a remote attacker could exploit this vulnerability to create requests that become larger than the threshold, and results in a denial of service condition.

CVEID: CVE-2022-35252 - cURL libcurl is vulnerable to a denial of service, caused by a flaw when cookies contain control codes are later sent back to an HTTP(S) server. By sending a specially-crafted request, a remote attacker could exploit this vulnerability to cause a "sister site" to deny service to siblings.

Affected Products and Versions

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

Link

PowerHA SystemMirror:

- **PowerHA SystemMirror support lifecycle information**

  This note lists the PowerHA SystemMirror release dates and end of service pack support (EoSPS) dates.

  Link

ESS updates:

- **Cumulative fixpacks with all fixes completed since the last release:**

- ESS_DAE_UNIFIED-6.1.5.1-ppc64LE-EM
  Link
- ESS_DME_UNIFIED-6.1.5.1-ppc64LE-EMS
  Link
- ESS_DAE_UNIFIED-6.1.5.1-x86_64-EMS
  Link
- ESS_VM-6.1.5.1-x86_64-EMS
  Link
- ESS_DME_UNIFIED-6.1.5.1-x86_64-EMS
  Link

Keep safe and remember to keep up to date!
Red, Belisama