Belisama

March Newsletter

Subscribe/Unsubscribe

Greetings all,
I trust that you all had a good first quarter of ‘24, a short break, and ready for the rest of challenging year as we juggle rising costs, tighter budget, with workloads and data that are continuing to grow. Some solace can be found in the fact that the tools and power ecosystem continue to evolve (more below), but there is more that can be done. I have been fortunate to have been asked to join in discussions with Power experts worldwide to look at how better solve IBM Power customer’s issues – and while I am across many – would welcome suggestions from any of my readers….

A few updates to share

- I have asked to present some papers at the TechXchange this year, so you should also be thinking about either presenting as well, or at least attending. It is currently scheduled for 21st to 24th October in Las Vegas (or possibly Florida) (Not 21-14 Oct as per IBM website). Important dates:
    - April 30 - session submission deadline
    - June 17 - accepted sessions announced
    - Late June - early view of the session catalog will be available late June

  Link
- We are looking at the Agenda for a Power User Group for ASEAN and ANZ and re-invigorating the existing meetup group – perhaps with the option of having some participants joining us in the IBM offices to participate – all suggestions welcome

In case you missed ….

- **Using emgr_check_ifixes on AIX 7.3**
  Chris Gibson explores using *emgr_check_ifixes* to automatically check for and download AIX security interim fixes.
  Link
- **What is Podman Desktop?**
  Part of the IBM Technology series looking at Podman Desktop - Container management and orchestration is critical part of software development of scalable applications, and Podman is here to help.
  Link
- **Migrating to AIX 7.3 with nimadm and Ansible**
  Chris Gibson explores using nimadm with Ansible to migrate an AIX LPAR from 7.2 to 7.3. Key to this functionality is the IBM AIX Ansible Galaxy collection, which includes the nim_alt_disk_migration Ansible role.
  Link
- **Ansible for IBM Power Overview**

Hariganesh Muralidharan gives an overview of Ansible on Power and looks at the recently added Ansible Lightspeed capability.
Link

- **PowerVM Performance Monitoring - Tips and Tricks for Grafana**
  Michal Wiktorek shares his tips for using Grafana to monitor IBM Power platform statistics, using the InfluxDB Data Source and Nigel Griffith's scripts, as well as some other options.
  Link
- **Upgrading the Power HMC with Ansible**
  A quick tutorial to Power HMC Upgrade with Ansible by Power DevOps
  Link

Redbooks and Redpapers

- **IBM Storage Scale System Introduction Guide (ESS)**, draft redpaper, 27 March 2024
  Link
- **IBM Storage Scale: Encryption**, Redpaper, 16 March 2024,
  Link

IBM alerts and notices

AIX alerts:

- **Highly Pervasive APAR IJ49737 Incorrect print queue status**
  An incorrect print queue status may be shown after a print job completes.

  Affected AIX Levels and Recommended Fixes (bos.rte.printers)

Min affected Level	Max affected Level	Fix Level	Interim Fix
7.2.5.202	7.2.5.202	7200-05-08	IJ49883
7.3.1.2	7.3.1.2	7300-01-04	IJ49914
7.3.2.0	7.3.2.0	7300-02-02	IJ49882

  Link

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

  CVE-2024-20952 - An unspecified vulnerability in Java SE related to the Security component could allow a remote attacker to cause high confidentiality impact and high integrity impact.
  CVE-2024-20918 - An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause high confidentiality impact and high integrity impact.
  CVE-2024-20921 - An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause high confidentiality impact.
  CVE-2024-20926 - An unspecified vulnerability in Java SE related to the Scripting component could allow a remote attacker to cause high confidentiality impact.

CVE-2024-20945 - An unspecified vulnerability in Java SE related to the VM component could allow a local authenticated attacker to cause high confidentiality impact.

CVE-2023-33850 - IBM GSKit-Crypto could allow a remote attacker to obtain sensitive information, caused by a timing-based side channel in the RSA Decryption implementation. By sending an overly large number of trial messages for decryption, an attacker could exploit this vulnerability to obtain sensitive information. IBM X-Force ID: 257132.

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 8.0.0.820

Link

- **AIX is vulnerable to security restrictions bypass due to cURL libcurl (CVE-2023-46218)**

Summary

Vulnerability in cURL libcurl could allow a remote attacker to bypass security restrictions (CVE-2023-46218). AIX uses cURL libcurl as part of rsyslog, LV/PV encryption integration with HPCS and in Live Update for interacting with HMC.

Vulnerability Details

CVE-2023-46218 - cURL libcurl could allow a remote attacker to bypass security restrictions, caused by a mixed case flaw when curl is built without PSL support. By sending a specially crafted request, an attacker could exploit this vulnerability to allow a HTTP server to set "super cookies" in curl.

Affected Products and Versions

Affected Product(s)	Version(s)
AIX	7.3.1
AIX	7.3.2

The following fileset levels are vulnerable:

Fileset	Lower Level	Upper Level
oss.lib.libcurl	7.79.1.0	7.79.1.0
oss.lib.libcurl	8.1.2.0	8.1.2.0

Note: This bulletin does not apply to versions of curl installed from the AIX Toolbox.

Link

- **AIX is vulnerable to a machine-in-the-middle attack (CVE-2023-48795), arbitrary command execution (CVE-2023-51385), and information disclosure (CVE-2023-51384) due to OpenSSH**

  Vulnerability Details

  CVE-2023-48795 - OpenSSH is vulnerable to a machine-in-the-middle attack, caused by a flaw in the extension negotiation process in the SSH transport protocol when used with certain OpenSSH extensions. A remote attacker could exploit this vulnerability to launch a machine-in-the-middle attack and strip an arbitrary number of messages after the initial key exchange, breaking SSH extension negotiation and downgrading the client connection security.

  CVE-2023-51385 - OpenSSH could allow a remote attacker to execute arbitrary commands on the system, caused by improper validation of shell metacharacters. By sending a specially crafted request using expansion tokens, an attacker could exploit this vulnerability to execute arbitrary commands on the system.

  CVE-2023-51384 - OpenSSH could allow a local authenticated attacker to obtain sensitive information, caused by a flaw when specifying destination constraints while adding PKCS#11-hosted private keys. 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.

  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
openssh.base.client	8.1.112.0	8.1.112.2000
openssh.base.server	8.1.112.0	8.1.112.2000
openssh.base.client	9.2.112.0	9.2.112.2000
openssh.base.server	9.2.112.0	9.2.112.2000

  Link

AIX technotes:

- **Capturing Debug Boot Output for AIX on Cloud**

  How to enable verbose (debug) output for AIX on Cloud during boot and capture it for later analysis by IBM. This is used by the customers who uses AIX on Cloud with the Service Broker Console.

[My Note: It still uses the horrid java console that IBM refuses to follow our requests and upgrade!! You you have limited ability to capture data, quick screenshots are probably your only option]
Link

- **What basic TCP tunings are recommended to improve performance of WAN connections between AIX virtual machines?**
  What basic TCP tunings are recommended to improve performance of WAN connections between AIX virtual machines?
  Link

- **The application on AIX is closing the idle connection sooner than expected. How to check the connection idle timeout used by the application?**
  The application on AIX is closing the idle connection sooner than expected. How to check the connection idle timeout used by the application?
  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.
  Link

- **Clarifying the path_status values when working with ALUA multi-path storage devices using AIX PCM (MPIO)**

Understanding of SCSI Asymmetric Logical Unit Access (ALUA) enabled devices is critical for ensuring a properly working multi-path storage configuration. The purpose of this document is to explain the extended 'path_status' values of the 'lsmpio' command to help system administrators understand if a storage path is either "selected" or "non-selected". ALUA is important as it allows for storage arrays to advertise which paths are available and preferred for host I/O.
Link

PowerSC alerts:

- **PowerSC is vulnerable to security restrictions bypass due to Curl (CVE-2023-46218, CVE-2023-46219, CVE-2024-0853**
  Vulnerability Details

  CVE-2023-46218 - cURL libcurl could allow a remote attacker to bypass security restrictions, caused by a mixed case flaw when curl is built without PSL support. By sending a specially crafted request, an attacker could exploit this vulnerability to allow a HTTP server to set "super cookies" in curl.
  CVE-2023-46219 - cURL libcurl could allow a remote attacker to bypass security restrictions, caused by a flaw when saving HSTS data to an

excessively long file name. By sending a specially crafted request, an attacker could exploit this vulnerability to use files that unaware of the HSTS status.
CVE-2024-0853 - cURL libcurl could allow a remote authenticated attacker to bypass security restrictions, caused by a flaw with keeping the SSL session ID for connections in its cache even when the verify status (OCSP stapling) test failed. By sending a specially crafted request, an attacker could exploit this vulnerability to bypass OCSP verification.

Affected Products and Versions

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

Link

ESS update:

- **New release information**
  - ESS_DAE_BASEIMAGE_3000-6.1.2.9-x86_64-Linux
  - ESS_DAE_BASEIMAGE_3200-6.1.2.9-x86_64-Linux

Keep safe and catch up in April
Red, Belisama