August Newsletter

Subscribe/Unsubscribe

Greetings all,
Trust that you are keeping well? Just a quick update (yes, late finishing my presentations for the TechXchange), but there is good news! There is likely to be a TechXchange in Australia later in the year – so if you not making it to Las Vegas, all is not lost.

A few updates to share

- September Techxchange
  Looks like a packed agenda and I will be covering the highlights in the September Newsletter. I was also pleased to see that Power and AIX have a strong presence – especially as Chris will be there running AIX hands on labs.
- VMRM cookbook
  Tim Simon and the editors have done a great job on tidying up our efforts, see below for details. The PowerHA cookbooks have been regularly top of the download lists – I hope this one will be as well received.
- AIX 7.3 vPMEM device support
  Need to use memory for high speed storage – and want it to persist across reboots?
  Link
- The future of computing requires advanced research in semiconductors today
  IBM and its partners are inventing what’s next in semiconductors.
  Link
- Did an AI write that? If so, which one? Introducing the new field of AI forensics
  IBM researchers are developing AI-text detection and attribution tools to make generative AI more transparent and trustworthy.
  Link

Quick bites

RedHat on Power
Just a quick (friendly!) reminder about need to upgrade:

- If you have P9 or P10 systems, you can upgrade to RHEL 9;
- If you have P8 systems, you can only go to RHEL 8; and
- If you have P7 or RHEL 7 BE, then you really need to move as BE linux is not supported anymore.

Plan it early and carefully to make this upgrade as boring as possible!

Simplify workstation deployments with Red Hat Enterprise Linux
A pretty handy blog from Gil Cattelain,
Link

Introducing the integration of IBM Power Virtual Server with IBM Key Protect for AIX and Linux
Great reading for organisations that want to encrypt their data in the cloud using their own encryption keys and retain control over and manage these keys
Link

Connecting IBM Virtual Private Cloud to IBM Power Virtual Servers and IBM Cloud Object Storage
This blog looks at connecting the robust IBM Power Virtual Servers service to the secure IBM Cloud Virtual Private Cloud environment using IBM Cloud to support diverse workloads.
Link

Coming soon

- **ASEANZK meetup**
  We are planning the next meetup at the end of September to have an in-depth look at the IBM Cloud Management Console.
  Spoiler alert: The IBM Cloud Management Console runs as a secure service hosted in the IBM cloud, designed to simplify maintaining software and monitoring and maintaining resources across on-premise, cloud or hybrid environments.

Redbooks and Redpapers

- **IBM Power E1080 Technical Overview and Introduction**, Redpaper, published: August 31, 2023
  Link
- **IBM Power S1014, S1022s, S1022, and S1024 Technical Overview and Introduction** , Redpaper, revised: August 31, 2023
  Link
- **IBM Power E1050: Technical Overview and Introduction** , Redpaper, revised: August 31, 2023
  Link
- **IBM Virtual Machine Recovery Manager for IBM Power Cookbook** , Redbook, published: August 18, 2023
  Link
- **IBM Power Virtual Server Guide for IBM AIX and Linux** , Redbook, published: August 12, 2023
  Link

IBM alerts and notices

AIX alerts:

- **Security Bulletin: CVE-2022-40609 affects IBM SDK, Java Technology**

  CVE-2022-40609 affects the Object Reqest Broker (ORB) in IBM SDK, Java Technology Edition.

  Vulnerability Details

  CVE-2022-40609 - IBM SDK, Java Technology Edition 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.

  Affected Products and Versions

Affected Product(s)	Version(s)
IBM SDK, Java Technology Edition	8.0.8.0 and earlier
IBM SDK, Java Technology Edition	7.1.5.18 and earlier

  Link

- **Security Bulletin: Multiple vulnerabilities affect IBM SDK, Java Technology**

  This bulletin covers all applicable Java SE CVEs published by Oracle as part of their July 2023 Critical Patch Update. For more information please refer to Oracle's July 2023 CPU Advisory and the X-Force database entries referenced below.

  Vulnerability Details

  CVE-2023-22045 - An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause low confidentiality impacts.

  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)
IBM SDK, Java Technology Edition	7.1.0.0 – 7.1.5.18 (restricted access)
IBM SDK, Java Technology Edition	8.0.0.0 - 8.0.8.6

  Link

- **AIX is affected by security restrictions bypass (CVE-2023-24329) due to Python**

  A vulnerability in Python could allow a remote attacker to bypass security restrictions (CVE-2023-24329). Python is used by AIX as part of Ansible node management automation.

  Vulnerability Details

  CVE-2023-24329 - Python could allow a remote attacker to bypass security restrictions, caused by a flaw in the urllib.parse component. By sending a specially-crafted request using URL starts with blank characters, an attacker could exploit this vulnerability to bypass blocklisting methods.

  Affected Products and Versions

Affected Product(s)	Version(s)
AIX	7.3

The following fileset levels are vulnerable:

Fileset	Lower Level	Upper Level
python3.9.base	3.9.0.0	3.9.16.0

Link

- **Security Bulletin: AIX is vulnerable to unauthorised file access and arbitrary code execution due to OpenSSH (CVE-2023-40371 and CVE-2023-38408)**

  Vulnerabilities in AIX's OpenSSH could allow a non-privileged local user file access outside of those allowed (CVE-2023-40371) or allow a remote attacker to execute arbitrary code (CVE-2023-38408). OpenSSH is used by AIX for remote login.

  Vulnerability Details

  CVE-2023-40371 - IBM AIX's OpenSSH implementation could allow a non-privileged local user to access files outside of those allowed due to improper access controls.

  CVE-2023-38408 - OpenSSH could allow a remote attacker to execute arbitrary code on the system, caused by a flaw in the forwarded ssh-agent. By sending specially crafted requests, 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

PowerVM alerts:

- **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.

  Link

- **Security Bulletin: AIX is vulnerable to unauthorised file access and arbitrary code execution due to OpenSSH**

  Vulnerabilities in AIX's OpenSSH could allow a non-privileged local user file access outside of those allowed (CVE-2023-40371) or allow a remote attacker to execute arbitrary code (CVE-2023-38408). OpenSSH is used by AIX for remote login.

  Vulnerability Details

  CVE-2023-40371 - IBM AIX's OpenSSH implementation could allow a non-privileged local user to access files outside of those allowed due to improper access controls.

CVE-2023-38408 - OpenSSH could allow a remote attacker to execute arbitrary code on the system, caused by a flaw in the forwarded ssh-agent. By sending specially crafted requests, 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

ESS/Scale alerts:

- **Kernel vulnerabilities could allow a denial of service**

  There are some vulnerabilities in the Linux kernel, used by IBM Elastic Storage System, which could allow a denial of service. Fixes for these vulnerabilities are available.

  Vulnerability Details

  CVE-2022-42703 - Linux Kernel is vulnerable to a denial of service, caused by a use-after-free flaw related to leaf anon_vma double reuse in mm/rmap.c. By sending a specially-crafted request, a local attacker could exploit this vulnerability to cause a denial of service.

  CVE-2022-4378 - Linux Kernel is vulnerable to a denial of service, caused by a stack-based buffer overflow in the __do_proc_dointvec function. By executing a specially-crafted program, a local authenticated attacker could exploit this vulnerability to cause a denial of service condition.

  Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale System	6.1.0.0 - 6.1.2.6
IBM Storage Scale System	6.1.3.0 - 6.1.8.0

  Link

- **Vulnerability in the Flask repo may affect affect IBM Elastic Storage System (CVE-2023-30861)**

  There is a vulnerability in the flask repo, used by IBM Elastic Storage System, which could allow a remote attacker to obtain sensitive information.

  Vulnerability Details

  CVE-2023-30861 - Pallets Flask could allow a remote attacker to obtain sensitive information, caused by missing Vary: Cookie header. By sending a specially crafted request, an attacker could exploit this vulnerability to obtain permanent session cookie information, and use this information to launch further attacks against the affected system.

  Affected Products and Versions

Affected Product(s)	Version(s)

IBM Storage Scale System	6.1.3.0 - 6.1.8.0

Link

- **A vulnerability in IBM WebSphere Application Server Liberty affects IBM Storage Scale packaged in IBM Elastic Storage Server (CVE-2023-24998)**

  There is a vulnerability in IBM WebSphere Application Server Liberty, used by IBM Elastic Storage Server, which could allow a remote attacker to cause a denial of service.

  Vulnerability Details

  CVE-2023-24998 - Apache Commons FileUpload and Tomcat are vulnerable to a denial of service, caused by not limit the number of request parts to be processed in the file upload function. By sending a specially-crafted request with series of uploads, a remote attacker could exploit this vulnerability to cause a denial of service condition.

  Affected Products and Versions

Affected Product(s)	Version(s)
IBM Elastic Storage Server	6.1.0.0 - 6.1.2.6
IBM Elastic Storage Server	6.1.3.0 - 6.1.6.1

  Link

- **Security Bulletin: Multiple Linux Kernel vulnerabilities may affect IBM Elastic Storage System**

  There are multiple vulnerabilities in the Linux kernel, used by IBM Elastic Storage System, which could allow a denial of service. Fixes for these vulnerabilities are available.

  Vulnerability Details

  CVE-2022-4269 - Linux Kernel is vulnerable to a denial of service, caused by a flaw in the Traffic Control (TC) subsystem. By using a specially-crafted networking configuration, a local authenticated attacker could exploit this vulnerability to cause a CPU soft lockup (ABBA deadlock), and results in a denial of service condition.

  CVE-2023-0461 - Linux Kernel could allow a local authenticated attacker to gain elevated privileges on the system, caused by a use-after-free bug of icsk_ulp_data of a struct inet_connection_sock. An attacker could exploit this vulnerability to gain elevated privileges on the system.

  Affected Products and Versions

Affected Product(s)	Version(s)
IBM Elastic Storage System	6.1.0.0 - 6.1.2.6
IBM Elastic Storage System	6.1.3.0 – 6.1.6.0

  Link

- **Security Bulletin: IBM Elastic Storage System is affected by a vulnerability in OpenSSL (CVE-2022-4450)**

  A security vulnerability has been discovered in OpenSSL.

  Vulnerability Details

CVE-2022-4450 - OpenSSL is vulnerable to a denial of service, caused by a double-free error related to the improper handling of specific PEM data by the PEM_read_bio_ex() function. By sending specially crafted PEM files for parsing, a remote attacker could exploit this vulnerability to cause the system to crash.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Elastic Storage System	6.1.0.0 - 6.1.2.6
IBM Elastic Storage System	6.1.3.0 – 6.1.8.0

Link

- **IBM Elastic Storage System: After upgrading to V6.1.8.0-6.1.8.1, ESS enabled with logtip/logtipback will cause continuous assert**

  IBM has identified an issue in IBM Elastic Storage System V6.1.8.0 through 6.1.8.1. This issue will cause continuous mmfsd daemon asserts after the upgrade in the case of a preexisting error condition with logtip or logtipback vdisk tracks.

  Prior to upgrading to ESS V6.1.8.0 or 6.1.8.1, if the logtip or logtipback vdisk tracks got into a condition where all the strips of the track are marked ‘stale’, recovery group continues to operation without functional issues. Under this condition, after upgrading to ESS V6.1.8.0 or 6.1.8.1, it will cause the mmfsd daemon to continuously assert before actions are taken.

  Users Affected:

  This issue can affect clients running IBM ESS prior to V6.1.8.0 (Scale V5.1.8.0), and intending to upgrade to ESS V6.1.8.0 (Scale V5.1.8.0) or 6.1.8.1 (Scale 5.1.8.1) with ESS storage configured with NVR and SSD DAs.

  Link

AIX informational:

- **AIX73 TL00 PTF in Error**

  Recommendation: - Update to AIX 7300-00-04-2320 or later

  Affected Filesets / Versions

MIN	MAX	FILESET
7.3.0.1	7.3.0.2	bos.rte.security
7.3.0.0	7.3.0.3	bos.net.tcp.client_core
7.3.0.0	7.3.0.4	bos.mp64

  Details:

  APAR: IJ44513 Fix available in service pack: 7300-00-04-2320

  Link

PowerVM informational:

- **PowerVM Virtual I/O Server**

  Now available:

  Software: Fix Pack: VIOS 3.1.3.40

Software: Fix Pack: VIOS 3.1.2.60

- **HMC Scanner for Power Server Configuration and Performance Stats**

  Update:

  You can 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 tool is available at the end of this document as a compressed file that needs to be extracted on an empty directory. Latest version is " hmcScanner-0.11.42.zip".

  Link

ESS / Scale / GPFS:

- **Cumulative updates**

  These fixpacks is cumulative and includes all fixes completed since the last release.

  Software: ESS_DAE_BASEIMAGE_3200-6.1.2.7-x86_64-Linux
  Software: ESS_DAE_BASEIMAGE_5000-6.1.2.7-ppc64LE-Linux
  Software: ESS_DAE_BASEIMAGE_Legacy-6.1.2.7-ppc64LE-Linux
  Software: ESS_DAE_BASEIMAGE_3000-6.1.2.7-x86_64-Linux
  Software: ESS_DME_BASEIMAGE_5000-6.1.2.7-ppc64LE-Linux
  Software: ESS_DME_BASEIMAGE_3200-6.1.2.7-x86_64-Linux
  Software: ESS_DME_BASEIMAGE_Legacy-6.1.2.7-ppc64LE-Linux
  Software: ESS_DME_BASEIMAGE_3000-6.1.2.7-x86_64-Linux
  Updates: ESS_VM-6.1.8.1-x86_64-UTILITY-EMS
  Updates: ESS_VM-6.1.8.1-x86_64-BYOE-EMS
  Updates: ESS_DAE_UNIFIED-6.1.8.1-ppc64LE-EMS
  Updates: ESS_DAE_UNIFIED-6.1.8.1-x86_64-EMS
  Updates: ESS_DME_UNIFIED-6.1.8.1-x86_64-EMS
  Updates: ESS_DME_UNIFIED-6.1.8.1-ppc64LE-EMS
  Updates: ESS_DAE_UNIFIED-6.1.8.2-x86_64-EMS
  Updates: ESS_VM-6.1.8.2-x86_64-UTILITY-EMS
  Updates: ESS_DAE_UNIFIED-6.1.8.2-ppc64LE-EMS
  Updates: ESS_VM-6.1.8.2-x86_64-BYOE-EMS
  Updates: ESS_DME_UNIFIED-6.1.8.2-ppc64LE-EMS
  Updates: ESS_DME_UNIFIED-6.1.8.2-x86_64-EMS
  Updates: ESS_FIRMWARE-6.1.8.2-ppc64LE-Linux
  Updates: ESS_FIRMWARE-6.1.8.2-x86_64-Linux

Save travels and hope to chat in Las Vegas.
Red, Belisama