Belisama

May Newsletter

Subscribe/Unsubscribe

Greetings all,
Trust you are keeping well – and hope to see lots of our Power Partners at the APAC Power Connect this week – hopefully many of the Sydney based ones in person.

A few updates to share

- Your **Power8 and end of Service** – are you looking at your options?
  Maintenance expiry dates:
  - 31/3/24: S812LC, S822, S822L, 822LC, 824 and 824L.
  - 31/5/24: S812L, S814 and 822LC.
  - 31/10/24: S821LC, S822LC, E850C, E870, E870C, E880 and E880C.
  - Mark McInnis has prepared a good summary of your options.

  Link
- VUG at TechXChange
  Another reason for attending the TechXchange in Vegas this year is that the PowerVUG will be held there, with Power product managers and other SMEs giving updates on all things Power related.
- The next VUG is entitled **S1012 and the Power Alternative for Your VMware / x86 Workloads**, with Presentations from:
  - Daniel Goldener, Product Manager of Scale-Out Power Systems
  - Bob Kovacs, Product Manager of Power Virtualisation
  - Todd Boyd, Power Systems Product Management

  Previous sessions can be found: http://ibm.biz/powersystemsvug
  Link
- **APAC Power Connect**, an IBM Australia Partner update, on 6/6/24, from 8:30 to 17:30 in the IBM George St Office.
  Speakers will include:
  - Bill Adra
  - Shannon Elwell
  - Jason Liu
  - Tonny Bastiaans
  - Ian Nash
  - Bruce Lai
  - Soumyojyoti Maitra
  - Simon Fennen

  Covering topics
  - Power Strategy 2024 Spotlight - Our Roadmap
  - Charging Tomorrow: AI on IBM Power
  - How We Win with PowerVS
  - PEP 2.0 highlights with HMC Scanner

- Competitive Take Out - VMWare Attack
- Riding the Wave: SAP HANA Market Insights
- Winning Formula: Mastering SAP HANA on Power in 2024
- Red Hat Open Hybrid Solutions on IBM Power Systems
- Modernisation Landscape for our clients
- PowerVS Private Update

Hope to see you there.
Link

Quick bites

Java SDK on AIX
IBM Support has updated a comprehensive web site with the latest information about Java SDK on AIX with details of supported versions, fixes, vulnerabilities and troubleshooting tips.
Link
IBM support published a technote: **What basic TCP tunings are recommended to improve performance of WAN connections between AIX virtual machines?**
Hint:

- tcp_sendspace=1048576 tcp_recvspace=1048576
- sb_max=2097152
- rfc1323=1
- tcp_nodelayack=0
- sack=1
- tcp_cubic=1
- mtu_bypass=on
- tcp_init_window=10

But see article for the full details.
Link

Call Home and Electronic Fix Distribution
Just a reminder that the public addresses are changing for the IBM servers that support Call Home and electronic download of fixes for customer systems' software, hardware, and operating system.
Link

HowTo: Step by step instructions to migrate a Virtual Media Library from a failing disk to another disk
IBM Support has published a guide on how to migrate a Virtual Media library from one disk to another.
Link

Active Directory (AD) on AIX : Step by step instructions to integrate Active Directory 2016 in AIX via LDAP protocol
IBM Support published this technote to explain the steps to configure user and group accounts of an Active Directory for Windows Server 2016 to be used as LDAP users and groups on the AIX operating system.
Link

PowerHA SystemMirror: How to remove a shared volume group from PowerHA cluster configuration.
IBM Support has published the general steps required to remove a shared Volume Group when it is no longer required for PowerHA or AIX
Link

Problem solving information: MustGather Testcase for VIOS Crash or VIOS Hang Condition
There are a range of different factors that can lead a VIOS partition to crash or hang. This may include, but it is not limited to, code defect or hardware malfunction. VIOS memory resource plays an important role in the VIOS availability and insufficient memory often leads to issues.
It is strongly recommended to read this document entirely before taking any actions to determine which scenario may be best applicable to your situation.
Link

Problem solving information: How to change cluster IP addresses in a single interface environment
This document published by IBM Support shows how to change the boot IP addresses of the cluster when is only 1 interface on the network
Link

Redbooks and Redpapers

- **IBM Storage Ceph Solutions Guide**, Redpaper: 30 May 2024
  Link
- **IBM Power S1012 Technical Overview and Introduction**, Draft Redpaper: 08 May 2024
  Link

IBM alerts and notices

AIX and PowerVM alerts:

Security Bulletin: AIX is vulnerable to arbitrary command execution due to invscout (CVE-2024-27260)
Summary
A vulnerability in the AIX invscout command could allow a non-privileged local user to execute arbitrary commands (CVE-2024-27260).

Vulnerability Details

IBM AIX could allow a non-privileged local user to exploit a vulnerability in the invscout command to execute arbitrary commands.

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
invscout.rte	2.2.0.0	2.2.0.26

Link

Security Bulletin: AIX is vulnerable to a denial of service due to libxml2 (CVE-2024-25062)

Summary

Vulnerability in libxml2 could allow a remote attacker to cause a denial of service (CVE-2024-25062). AIX uses libxml2 as part of its XML parsing functions.

Vulnerability Details

GNOME libxml2 is vulnerable to a denial of service, caused by a use-after-free flaw in the xmlValidatePopElement() function. By persuading a victim to open a specially crafted content, a remote attacker could exploit this vulnerability to cause the application to crash.

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
bos.rte.control	7.2.5.0	7.2.5.102
bos.rte.control	7.2.5.200	7.2.5.202
bos.rte.control	7.3.0.0	7.3.0.3
bos.rte.control	7.3.1.0	7.3.1.2
bos.rte.control	7.3.2.0	7.3.2.0

Link

Security Bulletin: AIX is vulnerable to privilege escalation (CVE-2024-27273)

Summary

Vulnerability in the AIX kernel may lead to privilege escalation (CVE-2024-27273).

Vulnerability Details

IBM AIX's Unix domain datagram socket implementation could potentially expose applications using Unix domain datagram sockets with SO_PEERID operation and may lead to privilege escalation.

Affected Products and Versions

Affected Product(s)	Version(s)
AIX	7.2
AIX	7.3
VIOS	3.1
VIOS	4.1

The vulnerabilities in the following filesets are being addressed:

Fileset	Lower Level	Upper Level
bos.mp64	7.2.5.0	7.2.5.107
bos.mp64	7.2.5.200	7.2.5.205
bos.mp64	7.3.0.0	7.3.0.5
bos.mp64	7.3.1.0	7.3.1.4
bos.mp64	7.3.2.0	7.3.2.1

Link

VMRM DR Alerts:

VMRM DR RC=83 error

There are a number of reasons that VMRM may encounter the RC=83 errors

- rehearsal fails
  In this instance the rehearsal discovery steps find extra Logical Units on the destination VIO(s)
  Link
- failure to move a VM due to storage or fabric switch configuration
  The move of a VM may fail and report an RC=83.
  Link

These documents cover several RC=83 errors, what needs to be checked and suggested recovery steps.

GPFS/Storage Scale and ESS Alerts:

Flashes: IBM Storage Scale V5.1.0.0 to V5.1.9.2: Undetected data and directory corruption: stale data may be read during "mmchdisk start" or left on disk

IBM has identified potential file system data integrity issues in file systems with data or metadata replication, including undetected data and directory corruption, with

IBM Storage Scale V5.1.0.0 to V5.1.9.2 (IBM Storage Scale System V6.1.0.0 to V6.1.9.2). Two different issues have been identified:

- Under some conditions, stale data can be read while the command "mmchdisk start" is run on file systems with replication.
- Stale data replicas may not get repaired by the "mmchdisk start" command.

Link

Flashes: HIPER: FlashCore Module (FCM) Critical update needed on FCMs on 3_x_x and 2_1_x Firmware

FCMs that are on 3_x_x and 2_1_x firmware will go offline if they have not had a firmware upgrade in the last 800 - 900 days.
It is imperative that FCMs on 2_1_11 and lower be updated to FCM 2_1_12 firmware IMMEDIATELY.

FCM FW	FW Release Date	800 days reached
2_1_2	1-Nov-2020	10-Jan-2023
2_1_3	15-Jan-2021	26-Mar-2023
2_1_4	22-Jun-2021	31-Aug-2023
2_1_5	09-Aug-2021	18-Oct-2023
2_1_6	12-Sep-2021	21-Nov-2023 (ESS Only)
2_1_10	23-Aug-2022	31-Oct-2024
2_1_11	15-Dec-2022	22-Feb-2025

It is important that FCMs on 3_1_7 and lower be updated to FCM 3_1_8 or 3_1_11 firmware in this first half of 2024

FCM FW	FW Release Date	800 days reached
3_0_1	1-Apr-2022	9-Jun-2024
3_1_2	19-Oct-2022	27-Dec-2024
3_1_4	14-Dec-2022	21-Feb-2025
3_1_7	20-Apr-2023	28-Jun-2025

Link

Security bulletin: Security Bulletin: Multiple vulnerabilities in IBM WebSphere Application Server Liberty affect IBM Storage Scale packaged in Elastic Storage Server.

Summary

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. CVE-2023-46158, CVE-2023-44487.

Vulnerability Details

IBM WebSphere Application Server Liberty 23.0.0.9 through 23.0.0.10 could provide weaker than expected security due to improper resource expiration handling. IBM X-Force ID: 268775.
CVE-2023-44487 - Multiple vendors are vulnerable to a denial of service, caused by a flaw in handling multiplexed streams in the HTTP/2 protocol. By sending numerous HTTP/2 requests and RST_STREAM frames over multiple

streams, a remote attacker could exploit this vulnerability to cause a denial of service due to server resource consumption.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Elastic Storage Server	6.1.0.0 - 6.1.2.8
IBM Elastic Storage Server	6.1.3.0 - 6.1.9.1

Link

Security bulletin: Security Bulletin: Multiple vulnerabilities in IBM WebSphere Application Server Liberty affects IBM Storage Scale packaged in IBM Storage Scale System

Summary

There are vulnerabilities in IBM WebSphere Application Server Liberty, used by IBM Storage Scale System GUI, which could allow a remote attacker to cause a denial of service.

Vulnerability Details

CVE-2023-22081 - An unspecified vulnerability in Java SE related to the JSSE component could allow a remote attacker to cause no confidentiality impact, no integrity impact, and low availability impact.
CVE-2023-22067 - An unspecified vulnerability in Java SE related to the CORBA component could allow a remote attacker to cause no confidentiality impact, low integrity impact, and no availability impact.
CVE-2023-5676 - Eclipse OpenJ9 is vulnerable to a denial of service, caused by a flaw when a shutdown signal (SIGTERM, SIGINT or SIGHUP) is received before the JVM has finished initializing. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause an infinite busy hang on a spinlock or a segmentation fault.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale System	6.1.0.0 - 6.1.2.8
IBM Storage Scale System	6.1.3.0 - 6.1.9.1

Link

Security bulletin: Security Bulletin: Multiple Linux Kernel vulnerabilities affects IBM Storage Scale packaged in IBM Storage Scale System.

Summary

There are multiple vulnerabilities in the Linux Kernel, used by IBM Storage Scale System, which could allow a denial of service. Fixes for these vulnerabilities are available. CVE-2023-5178, CVE-2023-3609, CVE-2023-45871, CVE-2023-4732, CVE-2023-1192.

Vulnerability Details

CVE-2023-5178 - Linux Kernel could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free flaw in the nvmet_tcp_free_crypto function in the NVMe-oF/TCP subsystem. By

sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary code on the system.
CVE-2023-3609 - Linux Kernel could allow a local authenticated attacker to gain elevated privileges on the system, caused by a use-after-free flaw in the net/sched: cls_u32 component. By sending a specially crafted request using the reference counter, an authenticated attacker could exploit this vulnerability to gain elevated privileges.
CVE-2023-45871 - Linux Kernel is vulnerable to a buffer overflow, caused by improper bounds checking by the IGB driver in drivers/net/ethernet/intel/igb/igb_main.c. By sending a specially crafted request, a remote attacker could overflow a buffer and execute arbitrary code or cause a denial of service condition on the system.
CVE-2023-4732 - Linux Kernel is vulnerable to a denial of service, caused by a race condition between task migrating pages and another task calling exit_mmap to release those same pages getting invalid opcode BUG in include/linux/swapops.h in the memory management subsytem. A local authenticated attacker could exploit this vulnerability to cause a denial of service.
CVE-2023-1192 - Linux Kernel is vulnerable to a denial of service, caused by a use-after-free flaw in the smb2_is_status_io_timeout() function in CIFS . By sending a specially crafted system call, a remote 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 - 6.1.2.8
IBM Storage Scale System	6.1.3.0 - 6.1.9.1

Link

GPFS/Storage Scale and ESS Flashes:

IBM Storage Scale Systems Alert: IBM Storage Scale System 6.1.8.2/6.1.9.x will no longer support IP over InfiniBand in "connected mode"

Customers will be unable to access IBM Storage Scale System in “connected mode” after upgrading to any of:

- MLNX_OFED version 23.07-0.5.0.0 or later on the client clusters
- IBM Storage Scale System 6.1.8.2 or 6.1.9.0 through 6.1.9.2 on the storage cluster

IPoIB Connected mode is no longer supported in that version of MLNX_OFED driver, and those IBM Storage Scale and System include a version of MLNX_OFED without the support.
Link

Keep safe and I will bother you again at the end of June
Red, Belisama