Belisama

July Newsletter

Subscribe/Unsubscribe

Greetings all,
I hope that the new financial year is off to a good start and you have caught up with IBM's latest updates for Partners and customers (if not check last months updates / send me an email)..

A few updates to share

- Work on presentations for IBM TechXchange Conference 2024 in Las Vegas from October 21-24 is proceeding and looking forward to catching up with Power users from around world – and hoping that there will be a good contingent from AP.
- In the checking phase for the AIX 7.3 Administrator Speciality exam, so hope that it will be available soon.

In case you missed ….

- **July VUG had some pretty cool announcements from Jayen Shah; Debbie Quick; Steve Finnes and Bob Kovacs:**
- AIX Updates
  - AIX 7.2 TL5 SP8
  - AIX 7.3 TL2 SP2
  - AIX 7.3 TL1 SP4
- PowerSC 2.2.0.1 updates
  - Compliance profile updates - The CIS compliance profile for RHEL 8 has been updated
  - Security updates:
    - Integration with IBM Safeguarded Copy
    - FIM enhancements on Linux with fapolicyd
    - TNC Enhancement to support NSF 4
    - Xcerces parser - added back into the package
    - Updates to the alerts configuration
    - Updates to the scheduler for compliance reports
- PowerSC 2.2.0.2
  - Compliance profile updates:
    - HIPPA compliance profile for AIX
    - CISv2 profile for RHEL
  - Security updates:
    - Filessystem directory hierarchy for logs, event, and data moved to /var
    - Ant-malware support for IBM i - integration with ClamAV
    - Updated alert structure
    - Profile-check scheduling from the UI
    - LDAP authorisation through PowerSC (without MFA)

  - MFA-managed user passwords for IBM i
  - HA-DR
- VMRM 1.8 Updates

Feature	Capability
SAP Netwearver Java	AIX support for NW has two options, ABAP and Java, this option extends VMRM HA support now also for the Java stack via agent
EMC RDF Group support	Enables seamless manage/unmanage VMs. Updating the RDF group used to be manual
GUI support for SPP	Manage shared processor pools via the GUI or cli
SAP HANA	vPMEM enables fast reload of VM memory after an outage
Storage replication	Enables customers to select Fibre Channel port
PowerVS DR (Q3 23)	VM recovery DR for AIX in PowerVS using GRS

- PowerHA 7.2.8 for AIX Updates

Feature	Capability
Fast recovery from ransomware attacks	PowerHA enabled CyberVault based on Safeguarded copies in Flash systems
Dedicated resource reservation in PowerVS	PowerHA AIX processor pool support in PowerVS integrating RoHA
HA and DR out of the box	PowerHA Std Ed AIX and VMRM DR integrate network IP management, so no script customisation required
PowerSC MFA HA	Smart Assist fro PowerSC MFA servers
Enhanced security for PowerHA / Oracle clustering	PowerHA support for Oracle encrypted volumes

- PowerHA 7.2.8 for AIX, SP1 and SP2

Feature	Capability
PowerHA in PowerVS	Single click configure and install of a Std Ed cluster
GLVM Synchronous mode	Two local copies of production data in PowerVS

- PowerHA 7.2.9 Q4 24

Feature	Capability
New generation Flash Storage	Replaces Global Mirror change volumes with Policy Replication for better RPO and eas of use
PowerHA will co-exist and migrate with Live Kernel Update and Live Library Update	PowerHA will tolerate and migrate alone with both LKU and LLU processes
Encryption for data at rest	Encryption for non-AIX LVM physical Volumes – eg Oracle ASM disk
Monitoring of non LVM disk	Enables failover in event of a disk fail for ASM
Code scan for final code distribution	Verify publisher identity

- Other deliverables:
  - FW version 1060 (14/06//24)
    - DDR5 memory
    - New I/O support
    - NVMe Drawer mulitpath
    - KVM on PowerVM
    - openSSL update
  - HMC / vHMC 10.3.1060 (14/06/24)
  - VIOS 4.1.0.21 (Servicepack) (07/06/24)

- VIOS 3.1.4.41 (Servicepack) (07/06/24)
  - New I/O
  - Fixes bundled / Service stream update
- PowerVC 2.2.1 (07/06/24)
  - Enhanced snapshot and quota
  - Dedicated hosts and Storage
  - Scaling of Hosts/Vms/Volumes
  - Standby hosts with add options
- Novalink 2.2.1 (07/06/24)
- HMC / vHMC
  - Support for above h/w updates
  - Sustainability metric reporting
  - Physical and virtual WWPN in call home data and predictive analysis
  - KVM on PowerVM enablement
- CMC 1.21 (07/06.24)
  - Patch level compliance checker
  - Infrastructure enhancements
  - Scaling and performance (96 systems in Pools 2.0)
  - Display subscription information in console

Replay
Slides

Coming soon

- **BM Cloud Management Console for Power Systems with Stephanie Jensen**

Upcoming session for the Power VUG (August 23/8 01:00AU; 22/8 23:00 SG)

The IBM Cloud Management Console (CMC) is a cloud-based service that provides clients with a complete as-a-service solution for their Power Systems environments. It can be accessed securely, anytime, anywhere to provide cross data centre monitoring. CMC is required for Power Private Cloud with Shared Utility Capacity, also known as Power Enterprise Pools 2.0 or PEP 2.0. PEP 2.0 provides the ability to group Power servers together in a pool to share processor, memory, and software license resources and pay for the use of the resources by the minute to optimise costs. CMC provides the following five applications:

Inventory	Aggregated and centralized inventory view with a dashboard for a quick status view
Capacity Monitoring	Aggregated system and partition performance views across your Power enterprise, including energy monitoring, shared processor pool metrics, and virtual network and storage metrics
Logging	Log aggregation and trends from Live Partition Mobility, Remote Restart, and partition lifecycle operations

Patch Planning	Current and latest update/upgrade views for system firmware, HMCs, I/O adapters, and AIX, IBM i, and Linux, along with the ability to create patch plans
Enterprise Pools 2.0	Deploy, monitor, and meter PEP 2.0 pools

This session will explore the CMC platform and apps in detail, and will include a live demo of all of the applications, including PEP 2.0.
Link

Redbooks and Redpapers

- **IBM Power 10 Scale Out Servers Technical Overview S1012, S1014, S1022s, S1022 and S1024**, Draft Redpaper, revised :04 July 2024
  Link
- **IBM Storage Ceph Concepts and Architecture Guide**, Redpaper, Published: 04 July 2024
  Link
- **SAP HANA on IBM Power Systems Architectural Summary**, Redpaper, Published 03 July 2024
  Link

IBM alerts and notices

AIX alerts:

- **AIX is vulnerable to a denial of service (CVE-2024-2511, CVE-2024-0727) due to OpenSSL**

Summary

Vulnerabilities in OpenSSL could allow a remote attacker to cause a denial of service (CVE-2024-2511, CVE-2024-0727). OpenSSL is used by AIX as part of AIX's secure network communications.

Vulnerability Details

CVE-2024-2511- OpenSSL is vulnerable to a denial of service, caused by improper server configuration validation. By using a specially crafted server configuration, a remote attacker could exploit this vulnerability to cause unbounded memory growth, and results in a denial of service condition.
CVE-2024-0727 - OpenSSL is vulnerable to a denial of service, caused by improper input validation. By persuading a victim to open a specially crafted PKCS12 file, 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
openssl.base	1.1.1.0	1.1.1.2200
openssl.base	1.1.2.0	1.1.2.2200
openssl.base	3.0.5.101	3.0.10.1002

Link

- **AIX is vulnerable to arbitrary code execution (CVE-2024-6387) due to OpenSSH**

Summary

Vulnerability in AIX's OpenSSH could allow a remote attacker to execute arbitrary code (CVE-2024-6387). OpenSSH is used by AIX for remote login.

Vulnerability Details

CVE-2024-6387 - OpenSSH could allow a remote attacker to execute arbitrary code on the system, caused by a signal handler race condition. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary code with root privileges on glibc-based Linux systems.

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	9.2.112.0	9.2.112.2400
openssh.base.server	9.2.112.0	9.2.112.2400

Link

AIX Updates:

- **Software: AIX Service Pack 7300-01-04-2420**

Service Packs contain important fixes and is based on Technology Level 7300-01.
Link

- **Downloads and drivers: 7300-01-04-2420**

AIX 7300-01 Service Pack 4
Link

PowerHA Updates:

- **PowerHA fix information for PowerHA 7.2.6 Service Pack 4**

PowerHA 7.2.6 Service Pack 4 is now available for download as of June 2024.
PowerHA SystemMirror 7.2.6 SP4 testing has been done on the following AIX levels and therefore they are recommended:

AIX7.3 TL02 SP2

AIX7.3 TL01 SP3
AIX7.3 TL00 SP4
AIX7.2 TL05 SP8
AIX7.2 TL04 SP6
AIX7.2 TL03 SP7
AIX7.2 TL02 SP6
AIX7.2 TL01 SP6
AIX7.1 TL05 SP12

Link

- **PowerHA fix information for PowerHA 7.2.7 Service Pack 2**
  PowerHA 7.2.7 Service Pack 2 is now available for download as of June 2024.
  PowerHA SystemMirror 7.2.7 SP2 testing has been done on the following AIX levels and therefore they are recommended:

  AIX7.3 TL02 SP2
  AIX7.3 TL01 SP3
  AIX7.3 TL00 SP4
  AIX7.2 TL05 SP8
  AIX7.2 TL04 SP6
  AIX7.2 TL03 SP7
  AIX7.2 TL02 SP6
  AIX7.2 TL01 SP6
  AIX7.1 TL05 SP12

  Link

- **PowerHA fix information for PowerHA 7.2.8 Service Pack 2**
  PowerHA 7.2.8 Service Pack 2 is now available for download as of June 2024.
  PowerHA SystemMirror 7.2.8 SP2 testing has been done on the following AIX levels and therefore they are recommended:

  AIX7.3 TL02 SP2
  AIX7.3 TL01 SP3
  AIX7.3 TL00 SP4
  AIX7.2 TL05 SP8
  AIX7.2 TL04 SP6
  AIX7.2 TL03 SP7
  AIX7.1 TL05 SP12

  Link

GPFS/Scale/ESS alerts:

- **An issue has been identified in Storage Scale System where buffer overflow problem is hit while getting FRU from drive FW table and that could result in a GPFS daemon crash**

The trigger for this problem would be somewhat random and it happens when GNR master node tries to fetch a FRU value from the drive FW table on all the paths. This race condition does not occur every time.
When this problem occurs, the GPFS daemon will crash. The /var/adm/ras/mmfs.log.latest will display something similar to the following messages:

```
024-04-24_10:15:15.842+1000: [I] Command: tschrecgroup --
recovery-group ALL --path-discovery enable
    *** buffer overflow detected ***: /usr/lpp/mmfs/bin/mmfsd
terminated
2024-04-24_10:15:16.115+1000: [E] Signal 6 at location
0x7F653B09EACF in process 1293717, link reg
0xFFFFFFFFFFFFFFFF.
2024-04-24_10:15:16.115+1000: [I] rax    0x0000000000000000
rbx    0x0000000000000006
```

Environment

This issue may affect clients running IBM Storage Scale System V6.1.7.0 to V6.1.9.2.

Link

- **Multiple vulnerabilities in IBM Java SDK affect IBM Storage Scale packaged in Elastic Storage Server**

Summary

There are multiple vulnerabilities in Java™ Technology Edition used by the Elastic Storage Server. Fixes for all these vulnerabilities are available. CVE-2024-20952, CVE-2024-20918, CVE-2024-20921, CVE-2024-20919, CVE-2024-20926, CVE-2024-20945.

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-2024-20919 - An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause high integrity 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.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Elastic Storage Server	6.1.0.0 - 6.1.9.2

Link

- **Multiple vulnerabilities in IBM JAVA JDK affect IBM Storage Scale packaged in IBM Storage Scale System**

Summary

Multiple vulnerabilities in IBM Java JDK, used by IBM Storage Scale System GUI, could allow an unauthenticated attacker to cause no confidentiality impact, low integrity impact and no availability impact. CVE-2024-20952, CVE-2024-20918, CVE-2024-20921, CVE-2024-20919, CVE-2024-20926, CVE-2024-20945.

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-2024-20919 - An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause high integrity 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.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale System	6.1.0.0 - 6.1.9.2

Link

- **In Storage Scale System(ESS) 3500 system, when upgrading NVMe drive firmware, the drive state can become 'missing', resulting in a firmware update failure.**

An unexpected behaviour in the hardware abstract layer (HAL) code can send unintended log page query to NVMe drives.

Details

The ESS Hardware Abstraction Layer (HAL) code monitors hardware statistics on regular basis. An unexpected behaviour has been identified in

HAL code which incorrectly issues a query to the NVMe drive. If an incorrect log page query happens to be issued during the restart phases within the NVMe drive firmware upgrade, the drive enters into a special state and becomes temporarily inaccessible, hence being marked as ‘missing’. As a result, a drive firmware upgrade failure could happen randomly and intermittently due to the described timing condition. NVMe drive firmware can be updated after multiple attempts.

Workaround:

Stop HAL service before running NVMe firmware upgrade:

```
# systemctl stop ibm-hal
```

Upgrade the NVMe drive firmware.

After the NVMe drive firmware upgrade completes, start HAL service again:

```
# systemctl start ibm-hal
```

Recommendation:

Customers that are affected should upgrade to IBM Storage Scale System V6.1.9.3 or V6.2.0.0 or later which is available on fix central:

Link

Keep safe and catch up in August with more updates..
Red, Belisama