Belisama

April Newsletter

Subscribe/Unsubscribe

Greetings all,
I hope that everyone is keeping well and had a good break with time to reflect and recharge, whether Easter or Eid.

A few updates to share

- Getting my sessions ready for this years TechXchange (Call for papers), hope you are also organising your travel/tickets!
- I was reminded recently about some of the extra features offered by FLRT (Fix Level Recommendation Tool). Not only is it a great tool for checking your Power environment (hardware, firmware, microcode, virtualisation, HMC…), prerequisites for new systems, LPM planning assistance, but there is the security vulnerability section. Details about AIX vulnerabilities/HYPERs can be download in a number of formats (eg csv). There is also a very useful project on git (link), which you can use to pull down lists of vulnerabilities by date range, score etc.
  Have a look at the data tables section for more information (link)

Quick bites

Five reasons to run Oracle workloads on IBM Power and IBM AIX

1. 33% lower application cost with Oracle Database SE2
2. ….

For details on how to save on software licensing (and the other 4 reasons) see:
Link

HMC Enhancements
An update on the new features and how it will help you manage your power environment, see the blog by Vijay Kumar Bana
Link

IBM Directory Server Installation on IBM AIX with Ansible
Installing IBM Security Directory Server will ease your user management, and Andrey Klyachkin shows how using Ansible.
Link

AIX automation – what is important for you?
Carl Burnett has invited us to have a say and let him know what we feel is important in AIX automation.
Link

List of handy metrics for GPFS/ESS?
IBM has updated the list of performance metrics available in the GPFS GUI, their description and a map to their corresponding mmperfmon metric name.
Link

IBM Power - Moving large files between systems
Diego Kesselman published a well written article to help customers move IBM Power workloads between local systems, data centres or to the Cloud.
Link

PowerHA SystemMirror
Support has updated the PowerHA SystemMirror support lifecycle information, which lists the PowerHA SystemMirror release dates and end of service pack support (EoSPS) dates.
Link

Redbooks and Redpapers

- **Recommendations for Implementing Geographic Logical Volume Manager (GLVM) On-Premises and on the Cloud**, Draft Redpaper, revised (already!) 16 April 2024
  Link

IBM alerts and notices

AIX alerts:

- **Why does the rpm command fail after I migrated to AIX 7.3 TL2?**
  Symptom:

```
 # rpm -qa
warning: Found bdb_ro Packages database while attempting
sqlite backend: using bdb_ro backend.
```

  Cause

  The rpm installer is an open source tool. IBM only packages it for AIX. The conversions from Berkely database to sqlite were forced by the RPM community.

  Link

Security Bulletin: AIX is vulnerable to arbitrary code execution due to RPM (CVE-2023-7104)

Summary

Vulnerability in RPM could allow a remote authenticated attacker to execute arbitrary code (CVE-2023-7104). RPM is used by AIX for package management.

Vulnerability Details

CVE-2023-7104 - SQLite SQLite3 is vulnerable to a heap-based buffer overflow, caused by improper bounds checking by the sessionReadRecord function in ext/session/sqlite3session.c. By sending a specially crafted request, a remote authenticated attacker could overflow a buffer and execute arbitrary code on the system.

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
rpm.rte	4.15.1.1000	4.15.1.1012
rpm.rte	4.15.1.2000	4.15.1.2010
rpm.rte	4.18.1.2000	4.18.1.2002

Link

Vulnerabilities in Python could allow a remote or local attacker to cause a denial of service (CVE-2023-52425, CVE-2023-52426) or launch further attacks on the system (CVE-2023-6597)

Summary

Vulnerabilities in Python could allow a remote or local attacker to cause a denial of service (CVE-2023-52425, CVE-2023-52426) or launch further attacks on the system (CVE-2023-6597). Python is used by AIX as part of Ansible node management automation.

Vulnerability Details

CVE-2023-52425 - libexpat is vulnerable to a denial of service, caused by improper system resource allocation. By sending a specially crafted request using an overly large token, a remote attacker could exploit this vulnerability to cause a denial of service.

CVE-2023-52426 - libexpat is vulnerable to a denial of service, caused by an XML entity expansion flaw if XML_DTD is undefined at compile time. By compiling specially crafted XML input, a local attacker could exploit this vulnerability to cause a denial of service.

CVE-2023-6597 - Python could provide weaker than expected security, caused by an issue with tempfile.TemporaryDirectory fails removing dir in some edge cases related to symlinks. A local attacker could exploit this vulnerability to launch further attacks on the system.

Affected Products and Versions

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

The following fileset levels are vulnerable:

Fileset	Lower Level	Upper Level
python3.9.base	3.9.0.0	3.9.18.1

Link

Software: Security Bulletin: AIX is vulnerable to email spoofing due to sendmail (CVE-2023-51765)

Summary

Vulnerability in sendmail could allow a remote attacker to spoof an email (CVE-2023-51765).

Vulnerability Details

CVE-2023-51765 - Proofpoint sendmail is vulnerable to SMTP smuggling, caused by improper handling of line endings . in an email message. By sending a specially crafted request using SMTP MAIL/RCPT/DATA commands, an attacker could exploit this vulnerability to spoof an email message from any MAIL FROM address.

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.net.tcp.sendmail	7.2.5.100	7.2.5.101
bos.net.tcp.sendmail	7.2.5.200	7.2.5.200
bos.net.tcp.sendmail	7.3.0.0	7.3.0.0
bos.net.tcp.sendmail	7.3.1.0	7.3.1.0
bos.net.tcp.sendmail	7.3.2.0	7.3.2.0

Link

PowerVM VIO Server alerts:

High Impact / Highly Pervasive APAR IJ50326 Unable to login as padmin after VIOS 4.1 upgrade

Abstract

Unable to login as padmin after VIOS 4.1 upgrade

Description

After an upgrade to VIOS 4.1.0.0 or VIOS 4.1.0.10, the padmin user may be unable to login due to premature password expiration.

When attempting to login from the console, the following error is displayed:

```
login: padmin
padmin's Password:
[compat]: 3004-327 Your password has been expired for toolong.
3004-321 Please see the system administrator to change your password.
```

When attempting to login from ssh, the following error is displayed:

```
padmin@vios2's password:
Permission denied, please try again.
```

Recommended Action

To avoid the issue, apply the ifix below before running viosupgrade. If the issue is hit, the padmin user attributes can be modified from HMC to allow login using:

```
# viosvrcmd -m <Managed System Name> --id <VIOS lpar id> -c "chuser -attr maxage=0 padmin"
# viosvrcmd -m <Managed System Name> --id <VIOS lpar id> -c "chuser -attr maxexpired=-1 padmin"
```

Affected VIOS Levels and Recommended Fixes

Min Affected Level	Max Affected Level	Fixing Level	iFix
VIOS 3.1.4.0 ios.cli.rte 7.2.5.200	VIOS 3.1.4.31 ios.cli.rte 7.2.5.205	VIOS 3.1.4.40	IJ50326
VIOS 3.1.3.0 ios.cli.rte 7.2.5.0	VIOS 3.1.3.40 ios.cli.rte 7.2.5.107	N/A	IJ50326

Link

VIOS_VFC_HOST with rc = 0x0000004F in error log

Symptom

```
LABEL:          VIOS_VFC_HOST
IDENTIFIER:     95A6D9B9
```

<snip>

Details

In this example, the return code 0x0000004F means the connection was refused. The VIOS request to login to storage port SCSI_ID <value>, not the switch port, was rejected (failure_type = 0x01 = LS_RJT) with reason being Unable to perform request (fail_reason_code = 0x09) and explanation as Command already in progress (fail_reason_exp = 0x19).

The "fp_ioctl() failed for SCIOLSTART" explains that operation for opening a logical path to the target device failed as above.

The most possible reason for getting such errors is that the storage believes there is another login still active, so this points more to the storage side.

Environment

VIOS 3.1

Resolving The Problem

Problem determination needs to be pursued from the storage side. Contact your local SAN Storage Support Representative and provide the storage port SCSI_ID <value(s)> the VIOS login request was rejected for, in this example, 0x0000000000020C00.

Link

Storage Scale Systems alerts:

A vulnerability in IBM WebSphere Application Server Liberty affects IBM Storage Scale packaged in IBM Storage Scale System

Summary

There is a vulnerability in IBM WebSphere Application Server Liberty, used by IBM Storage Scale System, which could allow a remote attacker to cause a denial of service. CVE-2023-46158, CVE-2023-44487

Vulnerability Details

CVE-2023-46158 - 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 Storage Scale System	6.1.x
IBM Storage Scale System	6.1.x

Remediation/Fixes

IBM recommends that you fix this vulnerability by upgrading affected versions of IBM Storage Scale System 3000, 3200, 3500, 5000 and 6000 to the following levels or higher:

V6.1.2.9 or later

V6.1.9.2 or later

Link

Vulnerability in libcurl may affect IBM Storage Scale System (CVE-2023-28322)

Summary

A vulnerability in libcurl may allow a remote attacker to bypass security restrictions in IBM Storage Scale System. A fix for this vulnerability is available.

Vulnerability Details

CVE-2023-28322 - cURL libcurl could allow a remote attacker to bypass security restrictions, caused by a flaw in the logic for a reused handle when it is (expected to be) changed from a PUT to a POST.. By sending a specially crafted request, an attacker could exploit this vulnerability to cause application to misbehave and either send off the wrong data or use memory after free or similar in the second transfer.

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

Remediation/Fixes

IBM recommends that you fix this vulnerability by upgrading affected versions of IBM Storage Scale System 3000, 3200, 3500 and 5000 to the following code levels or higher:

V6.1.2.9 or later
V6.1.9.2 or later

Link

Multiple Linux Kernel vulnerabilities may affect 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, an attacker to obtain sensitive information or gain elevated privileges on the system . Fixes for these vulnerabilities are available. CVE-2023-3772, CVE-2023-38409, CVE-2023-3567, CVE-2023-0458, CVE-2023-1075, CVE-2023-4622, CVE-2023-1073, CVE-2023-4128, CVE-2023-42753.

Vulnerability Details

CVE-2023-3772 - Linux Kernel is vulnerable to a denial of service, caused by a NULL pointer dereference flaw in the xfrm_update_ae_params() function in the IP framework for transforming packets (XFRM subsystem). By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause the kernel to crash.

CVE-2023-38409 - Linux Kernel is vulnerable to a denial of service, caused by a flaw in the set_con2fb_map function in drivers/video/fbdev/core/fbcon.c. By sending a specially crafted request, a local attacker could exploit this vulnerability to cause a denial of service condition.

CVE-2023-3567 - Linux Kernel could allow a local authenticated attacker to obtain sensitive information, caused by a use-after-free flaw in the vcs_read function in drivers/tty/vt/vc_screen.c in vc_screen. By sending a specially crafted request, an attacker could exploit this vulnerability to obtain internal kernel information or cause the system to crash.
CVE-2023-0458 -Linux Kernel could allow a remote authenticated attacker to obtain sensitive information, caused by a speculative pointer dereference in the do_prlimit() function. An attacker could exploit this vulnerability to leak the contents and obtain sensitive information.
CVE-2023-1075 - Linux Kernel could allow a local authenticated attacker to obtain sensitive information, caused by improper checking for list emptiness by the tls_is_tx_ready() function. By sending a specially crafted request to access a type confused entry to the list_head, an attacker could exploit this vulnerability to obtain the last byte of the confused field that overlaps with rec->tx_ready, and use this information to launch further attacks against the affected system.
CVE-2023-4622 - Linux Kernel could allow a local authenticated attacker to gain elevated privileges on the system, caused by a use-after-free flaw in the af_unix component. By sending a specially crafted request, an authenticated attacker could exploit this vulnerability to gain elevated privileges.
CVE-2023-1073 - Linux Kernel could allow a physical authenticated attacker to gain elevated privileges on the system, caused by a memory corruption flaw in the human interface device (HID) subsystem. By using a specially crafted USB device , an attacker could exploit this vulnerability to gain elevated privileges or cause a denial of service condition.
CVE-2023-4128 - Linux Kernel could allow a local authenticated attacker to gain elevated privileges on the system, caused by a use-after-free flaw in net/sched/cls_fw.c in classifiers. By sending a specially crafted request, an authenticated attacker could exploit this vulnerability to gain elevated privileges.
CVE-2023-42753 - Linux Kernel could allow a local authenticated attacker to execute arbitrary code on the system, caused by an integer underflow due to an array indexing issue in the netfilter ipset subsystem. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary code or 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

Remediation/Fixes

IBM recommends that you fix this vulnerability by upgrading affected versions of IBM Storage Scale System 3000, 3200, 3500, 5000, 6000 to the following code levels or higher:

V6.1.2.9 or later

V6.1.9.2 or later

Link

PowerHA SystemMirror updates:

PowerHA 7.2.5 Service Pack 6

PowerHA 7.2.5 Service Pack 6 is now available for download as of March 2024.

NOTE: PowerHA SystemMirror 7.2.5 SP6 testing has been done on the following AIX levels and are recommended:

- AIX7.3 TL02 SP1
- AIX7.3 TL01 SP3
- AIX7.3 TL00 SP4
- AIX7.2 TL05 SP7
- AIX7.2 TL04 SP6
- AIX7.2 TL03 SP7
- AIX7.2 TL02 SP6
- AIX7.2 TL01 SP6
- AIX7.1 TL05 SP12

Link

PowerHA 7.2.8 Service Pack 1

PowerHA 7.2.8 Service Pack 1 is now available for download as of March 2024.

NOTE: PowerHA SystemMirror 7.2.8 SP1 testing has been done on the following AIX levels and are recommended:

- AIX7.3 TL02 SP1
- AIX7.3 TL01 SP3
- AIX7.3 TL00 SP4
- AIX7.2 TL05 SP7
- AIX7.2 TL04 SP6
- AIX7.1 TL05 SP12

Link

Storage Scale Systems updates:

- ESS_DAE_BASEIMAGE_Legacy-6.1.2.9-ppc64LE-Linux
- ESS_DME_BASEIMAGE_3200-6.1.2.9-x86_64-Linux
- ESS_DME_BASEIMAGE_Legacy-6.1.2.9-ppc64LE-Linux
- ESS_DAE_BASEIMAGE_5000-6.1.2.9-ppc64LE-Linux
- ESS_DME_BASEIMAGE_5000-6.1.2.9-ppc64LE-Linux
- ESS_DME_BASEIMAGE_3000-6.1.2.9-x86_64-Linux

PowerVM VIO Server support updates:

HowTo: Step by step instructions to migrate a Virtual Media Library from a failing disk to another disk

Summary

This document provides step by step instructions on how to migrate a Virtual Media Library from a failing disk to another disk

Objective

While trying to replace a failing disk which contains a Virtual Media Library (VML), the standard approach to migrate the VML is to run the command

```
$ migratepv -lv VMLibrary hdisk0 hdisk1
```

Where:

hdisk0 represents the failing disk
hdisk1 represents the destination disk
VMLibrary represents the VML Logical Volume (LV)

In this scenario, since 'VMLibrary' is not an ordinary LV, the following output will be displayed

```
"VMLibrary" is a reserved name for the virtual media
repository.
```

Link

Keep safe and catch-up in May.
Red, Belisama