Belisama

June Newsletter

Subscribe/Unsubscribe

Greetings all,
Wishing you a successful end to the financial year (if the July – June financial year is your thing).
Has been a hectic year for us – so taking a short break for a couple of weeks.

A few updates to share

- Thanks to all those who joined my push to have trusted execution supported in the VIO Server – the idea status has now changed to delivered. From the initial install the trusted signature database will now also contain all the required signatures.
  In the background I am still pushing for a few more features to ensure that trusted execution is a bit tighter.
- IBM support has published a quick start guide for Oracle on Power10. Link
- IBM has put together a team that has started work preparing a new certification "IBM AIX v7.3 Administrator Speciality". Please let me know if there are any areas of AIX expertise we should be testing in this assessment.
- The Power Connect day in Sydney earlier this month was a great opportunity to catch up with other Power Partners and hear about some of the new opportunities for Power10 and what will be coming down the pipeline from IBM. The only shame was that there were not more partners to see that Power is still at the forefront.
- Using Ansible with AIX – some pointers from Andrey and Chris on creating Creating lpp_source with ansible Link
- New AIX releases:
  - 7300-02-02-2420
  - VIOS 4.1.0.21
  - VIOS 3.1.4.41

Quick bites

IBM Support update – "Using the Case page"
This update from support on 21/5/24, covers using the IBM Case page – displaying details about your cases, and make necessary changes. Some new features are also covered.
Link

In case you missed ….

- **The Power VUG on 20/6 "SAP HANA on IBM Power Systems"**
  Session replay
  S1012 Presentation Materials

Coming soon

- **IBM Power VUG - AIX SW bundles – Spring announcement**
  Join the next Power VUG for this exciting 90 minute session.
  Singapore 23:00 18/7; Sydney 01:00 19/7
  Link

Redbooks and Redpapers

- **IBM Power S1012 Technical Overview and Introduction**, Redpaper, revised: June 7, 2024
  Link

IBM alerts and notices

AIX and PowerVM alerts:

- **Multiple vulnerabilities in IBM Java SDK affect AIX**
  There are multiple vulnerabilities in IBM SDK Java Technology Edition, Version 8 used by AIX. AIX has addressed the applicable CVEs.
  Vulnerability Details
  CVE-2024-21085 - An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause low availability impacts.
  CVE-2023-38264 - The IBM SDK, Java Technology Edition's Object Request Broker (ORB) 7.1.0.0 through 7.1.5.21 and 8.0.0.0 through 8.0.8.21 is vulnerable to a denial of service attack in some circumstances due to improper enforcement of the JEP 290 MaxRef and MaxDepth deserialisation filters. IBM X-Force ID: 260578.
  Affected Products and Versions

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

  Link

- **AIX is affected by a denial of service due to Python (CVE-2024-0450)**

  Vulnerability in Python could allow a remote attacker to cause a denial of service (CVE-2024-0450). Python is used by AIX as part of Ansible node management automation.

  Vulnerability Details

  CVE-2024-0450 - Python CPython is vulnerable to a denial of service, caused by improper input validation by the zipfile module. By persuading a victim to open a specially crafted ZIP file, a remote attacker could exploit this vulnerability to cause a denial of service condition.

  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	3.9.18.3

  Link

- **AIX is affected by information disclosure due to Python (CVE-2024-28757)**

  Vulnerability in Python could allow a remote attacker to obtain sensitive information (CVE-2024-28757). Python is used by AIX as part of Ansible node management automation.

  Vulnerability Details

  CVE-2024-28757 - libexpat could allow a remote attacker to obtain sensitive information, caused by improper handling of XML external entity (XXE) declarations by the XML_ExternalEntityParserCreate function. By using a specially crafted XML content, a remote 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	7.3
VIOS	4.1

  The following fileset levels are vulnerable:

Fileset	Lower Level	Upper Level
python3.9.base	3.9.0.0	3.9.18.2

  Link

- **AIX is vulnerable to security restrictions bypass due to cURL libcurl (CVE-2024-0853)**

  Vulnerability in cURL libcurl could allow a remote attacker to bypass security restrictions (CVE-2024-0853). 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-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)
AIX	7.3 TL1 SP4
AIX	7.3 TL2 SP2

The following fileset levels are vulnerable:

Fileset	Lower Level	Upper Level
oss.lib.libcurl	8.5.0.0	8.5.0.0

Link

- **AIX is vulnerable to information disclosure due to openCryptoki (CVE-2024-0914)**

Vulnerability in openCryptoki could allow a remote attacker to obtain sensitive information (CVE-2024-0914).

Vulnerability Details

CVE-2024-0914 - openCryptoki could allow a remote attacker to obtain sensitive information, caused by a flaw when processing RSA PKCS#1 v1.5 padded ciphertexts. By utilize timing side-channel attack techniques, an attacker could exploit this vulnerability to obtain RSA ciphertext 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

Link

- **AIX is vulnerable to denial of service due to ISC BIND**

UPDATED: (Corrected the affected fileset levels to reflect that bind.rte 7.1.916.2604 and 7.3.916.2601 are vulnerable) Multiple vulnerabilities in ISC BIND could allow a remote attacker to cause a denial of service. AIX uses ISC BIND as part of its DNS functions.

Vulnerability Details

CVE-2023-50868 -ISC BIND is vulnerable to a denial of service, caused by an error when preparing an NSEC3 closest encloser proof. By flooding the target resolver with queries, a remote attacker could exploit this vulnerability to cause CPU exhaustion on a DNSSEC-validating resolver.

CVE-2023-50387 - Microsoft Windows is vulnerable to a denial of service, caused by improper restriction of DNSSEC verification complexity. By conducting an attack leveraging a highly complex DNSSEC verification

framework, a remote attacker could exploit this vulnerability to exhaust CPU resources and stall DNS resolvers, resulting in a denial of service.
CVE-2023-4408 - ISC BIND is vulnerable to a denial of service, caused by an error when parsing large DNS messages. By flooding the target server with queries, a remote attacker could exploit this vulnerability to cause excessive CPU load.
CVE-2023-6516 - ISC BIND is vulnerable to a denial of service, caused by an out-of-memory condition. By using specific recursive query patterns, a remote attacker could exploit this vulnerability to cause the amount of memory used by a named resolver to go well beyond the configured max-cache-size limit, leading to a denial of service.
CVE-2023-5679 - ISC BIND is vulnerable to a denial of service, caused by an error when enabling both DNS64 and serve-stale. By querying a DNS64-enabled resolver for domain names triggering serve-stale, a remote attacker could exploit this vulnerability to trigger an assertion failure.
CVE-2023-5517 - ISC BIND is vulnerable to a denial of service, caused by a flaw in query-handling code. By querying RFC 1918 reverse zones, a remote attacker could exploit this vulnerability to trigger an assertion failure.

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
bind.rte	7.1.916.0	7.1.916.2604
bind.rte	7.2.916.0	7.2.916.2600
bind.rte	7.3.916.0	7.3.916.2601

Link

PowerSC alerts:

- **PowerSC is vulnerable to security restrictions bypass and denial of service due to Curl**

PowerSC is vulnerable to security restrictions bypass and denial of service due to Curl

Summary

Vulnerabilities in Curl could allow a remote attacker to bypass security restrictions (CVE-2024-2466, CVE-2024-2004, CVE-2024-2379) or cause a denial of service (CVE-2024-2398). PowerSC uses Curl as part of PowerSC Trusted Network Connect (TNC).

Vulnerability Details

CVE-2024-2466 - cURL libcurl could allow a remote attacker to bypass security restrictions, caused by a flaw when built to use mbedTLS. By sending a specially crafted request, an attacker could exploit this vulnerability to bypass TLS certificate check.
CVE-2024-2004 - cURL libcurl could allow a local attacker to bypass security restrictions, caused by a lfaw in the logic for removing protocols. By sending a specially crafted request, an attacker could exploit this vulnerability to use the disabled set of protocols.
CVE-2024-2379 - cURL libcurl could allow a remote attacker to bypass security restrictions, caused by a flaw when wolfSSL library was built with the OPENSSL_COMPATIBLE_DEFAULTS symbol set. By sending a specially-crafted request, an attacker could exploit this vulnerability to bypass certificate verification for a QUIC connection.
CVE-2024-2398 - cURL libcurl is vulnerable to a denial of service, caused by a memory leak when allowing HTTP/2 server push. By sending a specially crafted PUSH_PROMISE frames with an excessive amount of headers, a remote attacker could exploit this vulnerability to cause a denial of service condition.

Affected Products and Versions

Affected Product(s)	Version(s)
PowerSC	1.3, 2.0, 2.1, 2.2

The vulnerabilities in the following filesets are being addressed:

Fileset	Lower Level	Upper Level
powerscStd.tnc_pm	1.3.0.4	2.2.0.2
curl-8.7.1-1.aix7.1.ppc.rpm	7.19.4	8.6.0

Link

ESS alerts:

- **Multiple PostgreSQL Vulnerabilities Affect IBM Storage Scale System**

Multiple PostgreSQL Vulnerabilities Affect IBM Storage Scale System
Summary

There are vulnerabilities in PostgreSQL versions used by IBM Storage Scale System that could allow a remote authenticated attacker to obtain sensitive information or bypass security restrictions, a denial of service and a buffer overflow. IBM Storage Scale System has addressed the applicable CVEs. CVE-2023-5868, CVE-2020-21469, CVE-2023-5869, CVE-2024-0985, CVE-2023-5870.

Vulnerability Details

CVE-2023-5868 - PostgreSQL could allow a remote authenticated attacker to obtain sensitive information, caused by a flaw when perform certain aggregate function calls. By sending a specially crafted request, an attacker could exploit this vulnerability to obtain bytes of server memory from the end

of the "unknown"-type value to the next zero byte, and use this information to launch further attacks against the affected system.
CVE-2020-21469 - PostgreSQL is vulnerable to a denial of service, caused by a buffer overflow. By sending specially crafted SIGHUP signals, a remote attacker could exploit this vulnerability to cause a denial of service condition.
CVE-2023-5869 - PostgreSQL is vulnerable to a buffer overflow, caused by improper bounds checking by the SQL array values. By sending a specially crafted request, a remote authenticated attacker could overflow a buffer and execute arbitrary code on the system.
CVE-2024-0985 - PostgreSQL could allow a remote authenticated attacker to bypass security restrictions, caused by a flaw when running in REFRESH MATERIALIZED VIEW CONCURRENTLY. By persuading a victim to run command a specially crafted view, an attacker could exploit this vulnerability to execute arbitrary SQL functions as the command issuer.
CVE-2023-5870 - PostgreSQL is vulnerable to a denial of service, caused by a flaw in the pg_signal_backend role. By sending a specially crafted request, 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 - 6.1.2.9
IBM Storage Scale System	6.1.3.0 - 6.1.9.2

Link

- **Multiple Linux Kernel vulnerabilities affect IBM Storage Scale System.**

There are multiple vulnerabilities in the Linux Kernel, used by IBM Storage Scale System, which could allow a local authenticated attacker to gain elevated privileges on the system. Fixes for these vulnerabilities are available. CVE-2023-51043, CVE-2024-1086, CVE-2024-0646, CVE-2023-6932, CVE-2024-26582, CVE-2023-6817.

Vulnerability Details

CVE-2023-51043 - Linux Kernel could allow a local authenticated attacker to gain elevated privileges on the system, caused by a use-after-free due to a race condition between a nonblocking atomic commit and a driver unload in drivers/gpu/drm/drm_atomic.c. By sending a specially crafted request, an authenticated attacker could exploit this vulnerability to gain elevated privileges.
CVE-2024-1086 - Linux Kernel could allow a local authenticated attacker to gain elevated privileges on the system, caused by use-after-free flaw in the nft_verdict_init() function in the Netfilter subsystem. By sending a specially crafted request, an authenticated attacker could exploit this vulnerability to gain elevated privileges.
CVE-2024-0646 - Linux Kernel could allow a local authenticated attacker to gain elevated privileges on the system, caused by an out-of-bounds memory write flaw in the Transport Layer Security functionality. A local attacker

could exploit this vulnerability to gain elevated privileges or cause the system to crash.
CVE-2023-6932 - Linux Kernel could allow a local authenticated attacker to gain elevated privileges on the system, caused by a use-after-free flaw in the ipv4: igmp component. By sending a specially crafted request, an authenticated attacker could exploit this vulnerability to gain elevated privileges.
CVE-2024-26582 - Linux Kernel could allow a local attacker to execute arbitrary code on the system, caused by a use-after-free flaw in the tls_decrypt_sg() function. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.
CVE-2023-6817 - Linux Kernel could allow a local authenticated attacker to gain elevated privileges on the system, caused by a use-after-free flaw in the nft_pipapo_walk function in the netfilter: nf_tables component. By sending a specially crafted request, an authenticated attacker could exploit this vulnerability to gain elevated privileges.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale System	6.1.0.0 - 6.1.2.9
IBM Storage Scale System	6.1.3.0 - 6.1.9.2

Link

ESS Planning:

- **IBM Storage Scale Software Version Recommendation Preventive Service Planning**
  IBM Storage Scale Software Version Recommendation
  This generalised recommendation is made available to assist clients in implementing a code update strategy. It is a full field perspective, and as such, a customized recommendation that takes into account specifics such as business upgrade windows, length of time since last update, decommission plans. might require assistance from local support teams. In general, recommendations assume planning updates annually.
  Link

Wishing you all a great start to the new financial year, and will catch up when back from Sri Lanka..

Antony Steel
Belisama