Belisama

June Newsletter

Subscribe/Unsubscribe

Greetings all,
I hope everyone is keeping safe and well – and looking forward to TechXchange in Las Vegas this year.

(Interesting stats: Some 3k sessions submitted; 190 Power related; 8 ASEAN and 48 ANZ – so there should be plenty of topics of interest for everyone.

Please let me know if you are interested in tickets – and I looking at travel options.
I have also heard a rumour that we may have a smaller version in ASEAN/ANZ later in the year, will update if confirmed.
As mentioned in the last newsletter, I am working on a GLVM paper, which has now been accepted as a Redpaper. I hope a draft will be ready by the end of July.

A few updates to share

- Thanks to Chris Gibson for reminding us that AIX 7.3 nimadm can migrate multibos enabled systems.
  Link
- Thanks to Anandakumar Mohan for an update covering:
  - Announcing Tech Preview of Red Hat Ansible Automation Platform on IBM
    Link
  - PowerSimplifying application deployment with OpenShift GitOps on IBM Power
    Link
  - Unleash IBM Power10 servers for accelerating AI model inferencing beyond GPUs!
    Link
- I have been assisting with a number of storage update and was reminded of the benefit of checking levels first. Make good use of the IBM System Storage Inter-operation Centre (SSIC)
  Link

Quick bites

Nigel's Blog
Don't forget this is a useful starting point when wanting to get a better understanding of AIX and the useful tools and performance monitoring. Has updated information on PowerVM, PowerVS, Linux on Power…
Link
GPFS
Don't forget that GPFS was rebranded IBM Spectrum Scale, which has now been rebranded to IBM Storage Scale. I still use the three product names interchangeably!

In case you missed ….

- **June PowerVUG**
  June's VUT covered the use of PowerHA with ROHA to provide a highly available deployment option for Oracle databases in an active/passive configuration on a pair of AIX LPARs on PowerVS
  Agenda:
  1. Power Virtual Server – Deploying AIX Instances
  2. ORACLE Database Installation Options with PowerHA
  3. PowerHA SystemMirror for AIX & Resource Optimized High Availability Feature
  4. Tips & Lessons Learned

  For this and previous sessions - Link
- **IBM Spectrum Scale Webinar – Installer Toolkit**
  IBM Spectrum Scale Webinars are hosted by IBM Spectrum Scale Support to share expertise and knowledge of the Spectrum Scale product, as well as product updates and best practices.
  This webinar focuses on the Installer Toolkit for IBM Spectrum Scale. See the agenda for more details. Note that our webinars are free-of-charge and held via Webex.
  Agenda
  1. Purpose/Why would I want to use the installation toolkit?
  2. Supported Features/Limitations
  3. Prerequisites
  4. Where can I get it?
  5. Where to start?
  6. Toolkit Phases
  7. Example Videos
  8. Trouble Shooting/Logs/Known issues
  9. Q&A

  For this and previous presentations see the link below.
  Audience: Spectrum Scale users and administrators
  Link

Coming soon

- **IBM TechXchange**
  Las Vegas 11-14 September

Redbooks and Redpapers

- **Implementing, Tuning, and Optimizing Workloads with Red Hat OpenShift on IBM Power**, Redboot, Published on 10 June 2023
  Link
- **Some interesting residencies coming up**
  - Update to SAP HANA on IBM Power Systems Architectural Summary
  - Automation with Ansible on Power

  Link

IBM alerts and notices

AIX and VIO alerts:

- **High Impact / Highly Pervasive APAR IJ46694 LDAP user logins or connections stop working**

  When reconnecting to an LDAP server, AIX and VIOS LPARs using LDAP authentication for users can experience an issue where the LDAP client daemon becomes unresponsive until it is restarted. This unresponsiveness can result in LDAP authenticated users being unable to login or existing LDAP connections to stop working.

  Affected Version / Level

  AIX 7300-01-02-2319
  AIX 7300-01-02-2320
  AIX 7300-01-03
  AIX 7200-05-06-2319
  AIX 7200-05-06-2320
  AIX 7200-05-07
  VIOS 3.1.4.20
  VIOS 3.1.4.21
  VIOS 3.1.4.30

  Link

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

  This bulletin covers all applicable Java SE CVEs published by Oracle as part of their April 2023 Critical Patch Update, plus CVE-2023-2597. For more information please refer to Oracle's April 2023 CPU Advisory and the X-Force database entries referenced below.

  Vulnerability Details

  CVE-2023-21930: An unspecified vulnerability in Oracle Java SE, Oracle GraalVM Enterprise Edition related to the JSSE component could allow an unauthenticated attacker to cause high confidentiality impact and high integrity impact.
  CVE-2023-21967: An unspecified vulnerability in Oracle Java SE, Oracle GraalVM Enterprise Edition related to the Hotspot component could allow a remote attacker to cause high confidentiality impact.
  CVE-2023-21954: An unspecified vulnerability in Oracle Java SE, Oracle GraalVM Enterprise Edition related to the JSSE component could allow a remote attacker to cause high availability impact.
  CVE-2023-21939: An unspecified vulnerability in Oracle Java SE, Oracle GraalVM Enterprise Edition related to the Swing component could allow a remote attacker to cause integrity impact.
  CVE-2023-21968: An unspecified vulnerability in Oracle Java SE and GraalVM Enterprise Edition related to the Libraries component could allow an unauthenticated attacker to cause low integrity impact.

CVE-2023-21937: An unspecified vulnerability in Oracle Java SE, Oracle GraalVM Enterprise Edition related to the Networking component could allow a remote attacker to cause integrity impact.
CVE-2023-21938: An unspecified vulnerability in Oracle Java SE, Oracle GraalVM Enterprise Edition related to the Libraries component could allow a remote attacker to cause integrity impact.
CVE-2023-2597: Eclipse Openj9 is vulnerable to a buffer overflow, caused by improper bounds checking by the getCachedUTFString() function. By using specially crafted input, a local authenticated attacker could overflow a buffer and execute arbitrary code on the system.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM SDK, Java Technology Edition	7.1.0.0 - 7.1.5.17
IBM SDK, Java Technology Edition	8.0.0.0 - 8.0.8.0\

Link

- **PowerSC Edition Security Bulletin**

There are multiple vulnerabilities in Curl that affect PowerSC.

Vulnerability Details

CVE-2023-27534: cURL libcurl could allow a remote attacker to obtain sensitive information, caused by a SFTP path ~ resolving discrepancy flaw. By sending a specially crafted request using a tilde (~) character, an attacker could exploit this vulnerability to obtain sensitive information from other directory, and use this information to launch further attacks against the affected system.
CVE-2022-43552: cURL libcurl is vulnerable to a denial of service, caused by a use-after-free flaw when using an HTTP proxy. By sending a specially-crafted request, a remote attacker could exploit this vulnerability to cause a denial of service condition.
CVE-2023-23914: cURL libcurl could allow a remote attacker to obtain sensitive information, caused by a flaw in the HSTS function when multiple URLs are requested serially. By sniffing the network traffic, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.
CVE-2023-23916: cURL libcurl is vulnerable to a denial of service, caused by a flaw in the decompression chain implementation. By sending a specially-crafted request, a remote attacker could exploit this vulnerability to cause memory errors, and results in a denial of service condition.
CVE-2023-27533: cURL libcurl could allow a remote attacker to bypass security restrictions, caused by a TELNET option IAC injection flaw. By sending a specially crafted request, an attacker could exploit this vulnerability to pass on user name and "telnet options" for the server negotiation.
CVE-2023-23915: cURL libcurl could allow a remote attacker to obtain sensitive information, caused by a flaw in the HSTS function when multiple URLs are requested in parallel. By sniffing the network traffic, an attacker

could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.
CVE-2023-27536: cURL libcurl could allow a remote attacker to bypass security restrictions, caused by a GSS delegation too eager connection re-use flaw. By sending a specially crafted request, an attacker could exploit this vulnerability to reuse a previously created connection even when the GSS delegation.
CVE-2022-43551: cURL libcurl could allow a remote attacker to bypass security restrictions, caused by a flaw when the host name in the given URL first uses IDN characters that get replaced to ASCII counterparts as part of the IDN conversion. By sending a specially-crafted request, an attacker could exploit this vulnerability to bypass HSTS check.
CVE-2023-27537: cURL libcurl is vulnerable to a denial of service, caused by a double free or use-after-free flaw when sharing HSTS data between separate "handles". By sending a specially crafted request, a remote attacker could exploit this vulnerability to cause a denial of service condition.
CVE-2023-27535: cURL libcurl could allow a remote attacker to bypass security restrictions, caused by a FTP too eager connection reuse flaw. By sending a specially crafted request, an attacker could exploit this vulnerability to reuse a previously created FTP connection.
CVE-2023-27538: cURL libcurl could allow a local attacker to bypass security restrictions, caused by a SSH connection too eager reuse still flaw. By sending a specially crafted request, an attacker could exploit this vulnerability to reuse a previously created connection even when an SSH related option had been changed.

All versions of PowerSC affected
Link

Informational:

- **Spectrum Scale / ESS updates**
  The following updates are now available
  Software: ESS_DME_UNIFIED-6.1.8.0-ppc64LE-EMS
  Link
  Software: ESS_DAE_UNIFIED-6.1.8.0-ppc64LE-EMS
  Link
  Software: ESS_VM-6.1.8.0-x86_64-EMS
  Link
  Software: ESS_DAE_UNIFIED-6.1.8.0-x86_64-EMS
  Link
  Software: ESS_DME_UNIFIED-6.1.8.0-x86_64-EMS
  Link

Keep safe and will send the next update around the end of July
Red, Belisama