Belisama

January Newsletter

Subscribe/Unsubscribe

Greetings all,
I hope that you all had a good break over the Western and Lunar New Years and ‘23 is off to a great start….

A few updates to share

- I have been fortunate to have been recognised by IBM and have been selected again as an IBM Champion for 2023. It is a great privilege and gives me access to the experts and details on coming updates and new features. Most of these I will be able to share once announced.
- Please join us for an IBM Product Briefing on “High Availability and Disaster Recovery using IBM Power Cloud – see below.

Quick bites

Resolve LVM commands throwing device configuration database query failed for vg
A new technote explains how to deal with the problem when LVM commands throw a message that the device configuration database query failed for vg.
For example when attempting varyonvg, you may get:

> 0516-1888 / mkvg error libodm: cannot open the object class collection file

Or when attempting to mkvg, you may get:

> 0519-100 libodm: Cannot open the object class collection file. Check path name and permissions.
> 0516-307 mkvg: Unable to access Device Configuration Database.

Link

Preparing customer firewalls and proxies for the upcoming infrastructure changes
This will affect IBM Call home and Electronic Fix Distribution
The Public IP addresses are changing for the IBM servers that support Call Home and electronic download of fixes for customer system's software, hardware, and operating system.
In particular addresses for esupport.ibm.com and www-945.ibm.com are changing.
Link

IBM Electronic support gateway servers ip address changes
This change is targeted for Q2 2023, and addresses for IBM Electronic support gateway servers eccgw01.boulder.ibm.com and eccgw02.rochester.ibm.com will be changing due to server migration to the Cloud.
Link

Coming soon

- **High Availability and Disaster Recovery using IBM Power Cloud**
  I will be presenting in Sydney and Canberra covering:
  - Introduction to PowerVS (Power in the IBM Cloud), looking at local availability features, and new options to manage license costs
  - DR options with the either the new Replication Service or GLVM
  - GLVM as an option to migrate to the cloud

  Sydney event:
  13 February, 15:30 – 17:00
  IBM Australia, Level 17, 259 George Street, Sydney, NSW 2000
  Register
  Canberra event:
  16 February, 15:30 – 17:00
  IBM Australia, Level 5, 28 Sydney Avenue, Forrest, ACT 2603
  Register

IBM alerts and notices

Security Bulletin:

- **AIX is vulnerable to denial of service vulnerabilities**
  Vulnerabilities in the AIX kernel and kernel extensions could allow a non-privileged local user to cause a denial of service (CVE-2022-43380, CVE-2022-40233, CVE-2022-39165, CVE-2022-43848, CVE-2022-43849, CVE-2022-39164).
  - A non-privileged local user could exploit a vulnerability in the AIX NFS kernel extension to cause a denial of service. IBM X-Force ID: 238640.
  - A non-privileged local user could exploit a vulnerability in the AIX TCP/IP kernel extension to cause a denial of service. IBM X-Force ID: 235599.
  - A non-privileged local user could exploit a vulnerability in CAA to cause a denial of service. IBM X-Force ID: 235183.
  - A non-privileged local user could exploit a vulnerability in the AIX perfstat kernel extension to cause a denial of service. IBM X-Force ID: 239169.
  - A non-privileged local user could exploit a vulnerability in the AIX pfcdd kernel extension to cause a denial of service. IBM X-Force ID: 239170.
  - A non-privileged local user could exploit a vulnerability in the AIX kernel to cause a denial of service. IBM X-Force ID: 235181.

Affected Product(s)	Version(s)
AIX	7.1
AIX	7.2
AIX	7.3
VIOS	3.1

  Link

- **AIX is vulnerable to a denial of service due to the AIX SMB client (CVE-2022-43381)**
  A vulnerability in the AIX SMB client daemon could allow a non-privileged local user to cause a denial of service (CVE-2022-43381).

Affected Product(s)	Version(s)
AIX	7.1
AIX	7.2
AIX	7.3
VIOS	3.1

  Link

- **AIX is vulnerable to a buffer overflow due to X11 (CVE-2022-47990)**
  A vulnerability in X11 on AIX could allow a non-privileged local user to cause a buffer overflow that could result in a denial of service or arbitrary code execution (CVE-2022-47990).

Affected Product(s)	Version(s)
AIX	7.1
AIX	7.2
AIX	7.3
VIOS	3.1

  Link

- **Multiple vulnerabilities in OpenSSL affect AIX**
  Vulnerabilities in OpenSSL could allow a remote attacker to cause a buffer overflow (CVE-2022-3062), cause a denial of service (CVE-2022-3786), or obtain sensitive information (CVE-2022-3358). OpenSSL is used by AIX as part of AIX's secure network communications.
  - OpenSSL is vulnerable to a stack-based buffer overflow, caused by improper bounds checking during X.509 certificate verification. By using a specially-crafted email address, a remote attacker could overflow a buffer and execute arbitrary code or cause the application to crash.
  - OpenSSL is vulnerable to a denial of service, caused by a stack based buffer overflow during X.509 certificate verification. By using a specially-crafted email address in a certificate, a remote attacker could exploit this vulnerability to cause a TLS client to crash, and results in a denial of service condition.
  - OpenSSL could allow a remote attacker to obtain sensitive information, caused by the improper handling of legacy custom ciphers passed to the EVP_EncryptInit_ex2(), EVP_DecryptInit_ex2() and EVP_CipherInit_ex2() functions. By creating a custom cipher with NID_undef using the legacy EVP_CIPHER_meth_new()function, a remote attacker could exploit this vulnerability force the use of a NULL cipher and emit the plain text as the cipher text.

Affected Product(s)	Version(s)
AIX	7.3.1

Link

Spectrum Scale:

- **IBM Spectrum Scale Software Version Recommendation Preventive Service Planning**
  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 customised 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

Keep safe and looking forward to working with you in ‘23
Red, Belisama