Belisama

December Newsletter

Subscribe/Unsubscribe

Greetings all,
Wishing you the best for the Western New Year and an interesting and happy ‘24. I tried to make this update short – but there were too many important updates/fixes that I didn’t want to leave out, so … Oh well, reading for January..

A few updates to share:

- An update on vPMEM with HANA on Power. Remember this no cost feature allows you to keep your large HANA database in memory while you stop HANA, reboot Linux and restart the LPAR.
  Link
- VIO 4.1 migration tips and insights (Ruchira Chawla). This update looks at the *viosupgrade* tool and some new features, including the preservation of device names and configurations.
  Link
- Overview of VIOS 4.1 (Rupesh Thota). This update covers many of the new features included in VIOS 4.1, which is built on AIX 7.3 TL2. These include security features, PV and LV encryption, long passwords, ksh93 as default, Python3, faster failover of fibre paths, improvements in CPU and memory DLPAR times, SSO rolling upgrades ….
  Link
- A timely reminder from Chris Gibson to refresh your AIX skills!
  - Mastering IBM AIX: Implementation and Administration (AN12G)
  - AIX Basics (AN10G)
  - Selection of badges

  With a selection of course based or virtual courses.
  Link
- Very glad to see the draft Redbook worked on by Hemantha “**Using Pacemaker to Create Highly Available Linux Solutions on IBM Power**” is now available (see below).

Quick bites

Waking up altinst_rootvg with the error code 0505-218
A problem can happen when executing *alt_rootvg_op -S* to put altinst_rootvg to sleep while the working directory is one of the filesystems related to the altinst_rootvg (/alt_inst/*), and then waking it up again using *alt_rootvg_op -Wd hdisk#* while still in that directory.
A number of errors may be seen relating to missing directories or Volume groups.
The altinst_rootvg VG missing after failed wakeup is fixed in APAR IJ47919 that was applied in the following versions:

Service Pack 7300-01-02-2320
Service Pack 7300-02-01-2346
Service Pack 7200-05-07-2346

Link

How to generate and collect a SNAP log archive needed by IBM Power Hardware Support from AIX or VIOS LRAR.

The support team has provided a timely reminder on how to generate and collect a SNAP archive and hopefully help reduce the time to resolution!

Link

SMS hangs when trying to display a list of bootable devices

A system with a large number of disks and large number of paths seems to hang when trying to display a list of bootable devices in SMS boot utility screens.

There are a number of ways to address this:

- Reduce the number of paths
- Specify the boot lun manually in SMS

Link

Error showing "mount: invalid argument"

Some uses have seen this error when attempting to mount a file system and is likely due to stanzas in the file system file not matching the LVCB of the logical volume.

Link

Stress test your AIX or Linux server with *nstress*

The stress package is a set of programs to keep many parts of the computer busy including CPU, memory, file systems, inter-process communications, and disks. Possible uses of the programs in the *nstress* toolbox are:

- You can "burn in" new hardware to prove it is reliable before production use;
- You can find out how fast your computer runs like memory speeds or disk I/O; and
- You can generate "fake" workloads and then use performance monitoring tools like *nmon* or *njmon* to see the performance stats in action.

Link

In case you missed ….

- **Webinar: Improve performance and accelerate business outcomes with AIX 7.3 TL updates.**

  IBM AIX Product Manager, Jayen Shah and Carl Burnet, DE for IBM Power, cover the latest enhancements on AIX 7.3 – How AIX OS feature enhancements provide the capacity, performance, and leading security needed to accelerate business outcomes and how to harness Power automation to stay current with the latest technology while keeping data secure and maintaining optimal performance

  Link

Coming soon

- **Introducing the IBM Storage Scale System 6000, on 11/1/24 at 01:00 SG; 04:00 AEST**
  IBM recently announced its newest IBM Storage Scale solution, the Storage Scale System (SSS) 6000. This new cloud-scale global data platform has the same ease-of-management as the ESS 3500, but with improved processing power, drive capacity, and performance. Join the Advanced Technology Group experts for this exciting session and overview on the newest member of the Storage Scale Family, the SSS 6000.
  Link

Redbooks and Redpapers

- **Using Pacemaker to Create Highly Available Linux Solutions on IBM Power**, Draft Redbook, updated 21 December 2023
  Link
- **Using Ansible for Automation with IBM Power Systems**, Draft Redbook, updated 21 December 2023
  Link
- **IBM Storage Ceph Solutions Guide**, Draft Redpaper, updated 29 November 2023
  Link

IBM alerts and notices

AIX alerts:

- **cfgdev / cfgmgr: 0514-621 WARNING: device packages not currently installed**
  The cfgmgr command (or cfgdev on VIOS) displays the following warning and fails to discover a new device:

  ```
  cfgmgr: 0514-621 WARNING: The following device packages are
  required for device support but are not currently installed.
  ```

  This message is followed by one or more fileset names such as:

  devices.fcp.disk
  devices.fcp.changer
  devices.fcp.tape
  devices.sas.changer

  Link

AIX Security Bulletins:

- **AIX is vulnerable to privilege escalation and denial of service (CVE-2023-45166, CVE-2023-45174, CVE-2023-45170)**
  A vulnerability in the AIX printers system could allow a non-privileged local user to obtain elevated privileges or cause a denial of service (CVE-2023-45166, CVE-2023-45174, CVE-2023-45170).
  Vulnerability Details

CVEID: CVE-2023-45166 - IBM AIX could allow a non-privileged local user to exploit a vulnerability in the piodmgrsu command to obtain elevated privileges.
CVEID: CVE-2023-45174 - IBM AIX could allow a privileged local user to exploit a vulnerability in the qdaemon command to escalate privileges or cause a denial of service.
CVEID: CVE-2023-45170 - IBM AIX could allow a non-privileged local user to exploit a vulnerability in the piobe command to escalate privileges or cause a denial of service.

Affected Products and Versions

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

Link

- **Multiple vulnerabilities in cURL libcurl affect AIX**

Multiple vulnerabilities in cURL libcurl affect AIX. AIX uses cURL libcurl as part of LV/PV encryption integration with HPCS and in Live Update for interacting with HMC.

Vulnerability Details

CVEID: CVE-2023-38546 - cURL libcurl could allow a remote attacker to bypass security restrictions, caused by a flaw in the curl_easy_duphandle function if a transfer has cookies enabled when the handle is duplicated. By sending a specially crafted request, an attacker could exploit this vulnerability to insert cookies at will into a running program.
CVEID: CVE-2023-38545 - libcurl and cURL are vulnerable to a heap-based buffer overflow, caused by the improper handling of hostnames longer than 255 bytes during a slow SOCKS5 proxy handshake. By sending an overly long argument, a remote attacker could overflow a buffer and execute arbitrary code on the system.

Affected Products and Versions

Affected Product(s)	Version(s)
AIX	7.3.1
AIX	7.3.2

Link

- **AIX is vulnerable to arbitrary command execution due to invscout (CVE-2023-45168)**

A vulnerability in the AIX invscout command could allow a non-privileged local user to execute arbitrary commands (CVE-2023-45168).

Vulnerability Details

CVEID: CVE-2023-45168 - IBM AIX could allow a non-privileged local user to exploit a vulnerability in the invscout command to execute arbitrary commands.

Affected Products and Versions

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

Link

- **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

CVEID: CVE-2023-22081 - An unspecified vulnerability in Oracle Java SE, Oracle GraalVM for JDK related to the JSSE component could allow a remote attacker to cause no confidentiality impact, no integrity impact, and low availability impact.

CVEID: CVE-2023-22067 - An unspecified vulnerability in Oracle Java SE related to the CORBA component could allow a remote attacker to cause no confidentiality impact, low integrity impact, and no availability impact.

CVEID: CVE-2023-5676 - Eclipse OpenJ9 is vulnerable to a denial of service, caused by a flaw when a shutdown signal (SIGTERM, SIGINT or SIGHUP) is received before the JVM has finished initializing. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause an infinite busy hang on a spinlock or a segmentation fault.

Affected Products and Versions

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

Link

- **AIX is vulnerable to denial of service due to ISC BIND (CVE-2023-3341)**

A vulnerability in ISC BIND could allow a remote attacker to cause a denial of service (CVE-2023-3341) AIX uses ISC BIND as part of its DNS functions.

Vulnerability Details

CVEID: CVE-2023-3341 - ISC BIND is vulnerable to a denial of service, caused by a stack exhaustion flaw in control channel code. By sending a specially crafted message over the control channel, a remote attacker could exploit this vulnerability to cause named to terminate.

Affected Products and Versions

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

Link

- **AIX is vulnerable to denial of service due to AIXWindows (CVE-2023-45172)**
  A vulnerability in AIXwindows could allow a non-privileged local user to cause a denial of service (CVE-2023-45172).
  Vulnerability Details
  CVEID: CVE-2023-45172 - IBM AIX could allow a non-privileged local user to exploit a vulnerability in AIXwindows to cause a denial of service.
  Affected Products and Versions

Affected Product(s)	Version(s)
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-2023-45165)**
  A vulnerability in the AIX SMB client daemon could allow a non-privileged local user to cause a denial of service (CVE-2023-45165). AIX uses the SMB client daemon to access files on SMB servers.
  Vulnerability Details
  CVEID: CVE-2023-45165 - IBM AIX could allow a non-privileged local user to exploit a vulnerability in the AIX SMB client to cause a denial of service.
  Affected Products and Versions

Affected Product(s)	Version(s)
AIX	7.2
AIX	7.3

  Link

- **AIX is affected by multiple vulnerabilities due to Python (CVE-2023-43804, CVE-2023-37920)**
  Vulnerabilities in Python could allow a remote authenticated attacker to obtain sensitive information (CVE-2023-43804). AIX's Python packaging also includes Certifi, which is vulnerable to CVE-2023-37920. Python is used by AIX as part of Ansible node management automation.
  Vulnerability Details
  CVEID: CVE-2023-43804 - urllib3 could allow a remote authenticated attacker to obtain sensitive information, caused by a flaw with cookie request

header not stripped during cross-origin redirects. By sending a specially crafted request, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.
CVEID: CVE-2023-37920 - An unspecified error with the removal of e-Tugra root certificate in Certifi has an unknown impact and attack vector.

Affected Products and Versions

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

Link

PowerSC Security Bulletins:

- **Multiple vulnerabilities in Curl affect PowerSC**

There are multiple vulnerabilities in Curl that affect PowerSC. PowerSC uses Curl as part of PowerSC Trusted Network Connect (TNC).

Vulnerability Details

CVEID: CVE-2023-38039 - cURL libcurl is vulnerable to a denial of service, caused by not limiting the number and size of headers accept in a response. By sending a specially crafted request, a remote attacker could exploit this vulnerability to run out of heap memory, and results in a denial of service condition.
CVEID: CVE-2023-38546 - cURL libcurl could allow a remote attacker to bypass security restrictions, caused by a flaw in the curl_easy_duphandle function if a transfer has cookies enabled when the handle is duplicated. By sending a specially crafted request, an attacker could exploit this vulnerability to insert cookies at will into a running program.
CVEID: CVE-2023-38545 - libcurl and cURL are vulnerable to a heap-based buffer overflow, caused by the improper handling of hostnames longer than 255 bytes during a slow SOCKS5 proxy handshake. By sending an overly long argument, a remote attacker could overflow a buffer and execute arbitrary code on the system.

Affected Products and Versions

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

Link

ESS Security Bulletins:

- **There are some vulnerabilities in the Linux kernel, used by IBM Elastic Storage System, which could allow a denial of service**

Vulnerability Details

CVEID: CVE-2023-32233 - Linux Kernel could allow a local authenticated attacker to gain elevated privileges on the system, caused by a use-after-free flaw in Netfilter nf_tables when processing batch requests. By sending a specially crafted request, an authenticated attacker could exploit this vulnerability to gain elevated privileges as root.
CVEID: CVE-2023-2124 - Linux Kernel could allow a local authenticated attacker to gain elevated privileges on the system, caused by an out-of-bounds access flaw in the XFS subsystem due to a missing metadata validation when mounting a user-supplied XFS disk image. By sending a specially crafted request, an authenticated attacker could exploit this vulnerability to gain elevated privileges or cause a denial of service condition.
CVEID: CVE-2023-1637 - Linux Kernel could allow a local authenticated attacker to obtain sensitive information, caused by a flaw in the X86 CPU Power management options function. By sending a specially crafted request, an attacker could exploit this vulnerability to obtain sensitive information in the memory of the CPU, and use this information to launch further attacks against the affected system.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Elastic Storage System	6.1.0.0 - 6.1.2.7
IBM Elastic Storage System	6.1.3.0 - 6.1.8.2

Link

- **IBM Elastic Storage System is shipped with GNU glibc, for which a fix is available for a security vulnerability.**

Vulnerability Details

CVEID: CVE-2023-4911 - glibc could allow a local authenticated attacker to gain elevated privileges on the system, caused by a buffer overflow in the dynamic loader's processing of the GLIBC_TUNABLES environment variable. By sending overly long data, an attacker could exploit this vulnerability to gain root privileges on the system.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Elastic Storage System	6.1.0.0 - 6.1.2.7
IBM Elastic Storage System	6.1.3.0 - 6.1.8.2

Link

- **There is a vulnerability in the Linux kernel, used by IBM Elastic Storage System, which could allow a denial of service.**

Vulnerability Details

CVEID: CVE-2023-28466 - Linux Kernel is vulnerable to a denial of service, caused by the lack of a lock_sock call in do_tls_getsockopt in net/tls/tls_main.c. By sending a specially crafted request, a local attacker

could exploit this vulnerability to cause a race condition, and results in a denial of service condition.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Elastic Storage System	6.1.0.0 - 6.1.2.7
IBM Elastic Storage System	6.1.3.0 - 6.1.8.2

Link

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

There are vulnerabilities in the Linux kernel, used by IBM Storage Scale System, which could allow a denial of service. Fixes for these vulnerabilities are available.

Vulnerability Details

CVEID: CVE-2023-1195 - Linux Kernel is vulnerable to a denial of service, caused by a use-after-free flaw in the reconn_set_ipaddr_from_hostname function in fs/cifs/connect.c. By sending a specially crafted request, a remote authenticated attacker could exploit this vulnerability to cause a denial of service condition.

CVEID: CVE-2022-3567 - Linux Kernel is vulnerable to a denial of service, caused by a race condition flaw in the inet6_stream_ops/inet6_dgram_ops function in the IPv6 Handler. By sending a specially crafted request, a remote authenticated attacker could exploit this vulnerability to cause a denial of service condition.

CVEID: CVE-2023-0394 - Linux Kernel s vulnerable to a denial of service, caused by a NULL pointer dereference flaw in the rawv6_push_pending_frames function in net/ipv6/raw.c. By sending a specially-crafted request, a remote authenticated attacker could exploit this vulnerability to cause the system to crash.

CVEID: CVE-2022-0854 - Linux Kernel could allow a local authenticated attacker to obtain sensitive information, caused by memory leak flaw in the DMA subsystem. By sending a specially-crafted request using the DMA_FROM_DEVICE function, an attacker could exploit this vulnerability to read random memory from the kernel space, and use this information to launch further attacks against the affected system.

CVEID: CVE-2023-4004 - Linux Kernel could allow a local authenticated attacker to gain elevated privileges on the system, caused by a flaw in the nft_pipapo_remove function in the netfilter. By sending a specially crafted request, an authenticated attacker could exploit this vulnerability to gain elevated privileges or cause the system to crash.

CVEID: CVE-2022-1184 - Linux Kernel is vulnerable to a denial of service, caused by a use-after-free flaw in the dx_insert_block() function in in fs/ext4/namei.c. By sending a specially-crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service condition.

CVEID: CVE-2022-47929 - Linux Kernel is vulnerable to a denial of service, caused by a NULL pointer dereference in the traffic control

subsystem. By using specially crafted traffic control configuration that is set up with "tc qdisc" and "tc class" commands, a local attacker could exploit this vulnerability to cause the system to crash.
CVEID: CVE-2023-35001 - Linux Kernel could allow a local authenticated attacker to gain elevated privileges on the system, caused by a nf_tables nft_byteorder_eval out-of-bounds read/write. By sending a specially crafted request, an aattacker could exploit this vulnerability to escalate privileges.
CVEID: CVE-2022-0168 - Linux Kernel is vulnerable to a denial of service, caused by a NULL pointer dereference flaw in the smb2_ioctl_query_info function in the fs/cifs/smb2ops.c. By sending a specially-crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service condition.
CVEID: CVE-2022-3566 - A race condition in the function tcp_getsockopt/tcp_setsockopt of the component TCP Handler in Linux Kernel could allow a remote authenticated attacker from within the local network to cause an unknown impact.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale System	6.1.0.0 - 6.1.2.7
IBM Storage Scale System	6.1.3.0 - 6.1.8.3

Link

- **Multiple security vulnerabilities in systemd may affect IBM Storage Scale System**

Multiple security vulnerabilities has been identified in IBM Storage Scale System where systemd is vulnerable to denial of service. A fix for these vulnerabilities is available.

Vulnerability Details

CVEID: CVE-2022-4415 - systemd could allow a local authenticated attacker to obtain sensitive information, caused by not respecting fs.suid_dumpable kernel setting in the systemd-coredump. By sending a specially-crafted request, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.
CVEID: CVE-2022-3821 - systemd is vulnerable to a denial of service, caused by an off-by-one error in format_timespan() function of time-util.c. By sending specific values for time and accuracy, a local attacker could exploit this vulnerability to cause a denial of service.
CVEID: CVE-2023-26604 - systemd could allow a local authenticated attacker to gain elevated privileges on the system, caused by the failure to set LESSSECURE to 1 in the configurations. By sending a specially crafted request, an attacker could exploit this vulnerability to gain root privileges on the system.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale System	6.1.0.0 - 6.1.2.7
IBM Storage Scale System	6.1.3.0 - 6.1.8.3

Link

- **glibc vulnerability may affect IBM Storage Scale System (CVE-2023-4806)**
IBM Storage Scale System is shipped with GNU glibc, for which a fix is available for a security vulnerability.
Vulnerability Details
CVEID: CVE-2023-4806 - GNU glibc is vulnerable to a denial of service, caused by a use-after-free flaw in the getaddrinfo() function. By sending a specially crafted request, a remote attacker could exploit this vulnerability to cause the application to crash.
Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale System	6.1.0.0 - 6.1.2.7
IBM Storage Scale System	6.1.3.0 - 6.1.8.3

Link

- **Multiple vulnerabilities in Python may affect the IBM Storage Scale System**
Multiple security vulnerabilities have been identified in IBM Storage Scale System where Python is vulnerable to denial of service. Fixes for these vulnerabilities are available.
Vulnerability Details
CVEID: CVE-2022-45061 - Python is vulnerable to a denial of service, caused by an unnecessary quadratic algorithm exists in one path when processing some inputs to the IDNA (RFC 3490) decoder. By sending a specially-crafted input, a remote attacker could exploit this vulnerability to cause a CPU denial of service condition.
CVEID: CVE-2020-10735 - Python is vulnerable to a denial of service, caused by the failure to limit amount of digits converting text to int by the int() type in PyLong_FromString(). A remote attacker could exploit this vulnerability to consume all available resources.
CVEID: CVE-2023-40217 - Python could allow a remote attacker to bypass security restrictions, caused by a race condition in the SSLSocket module. When the socket is closed before the TLS handshake is complete, the data is treated as if it had been encrypted by TLS. An attacker could exploit this vulnerability to bypass the TLS handshake and inject a malicious client certificate into the connection and gain access to the server’s resources without being authenticated.
Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale System	6.1.0.0 - 6.1.2.7
IBM Storage Scale System	6.1.3.0 - 6.1.8.3

Link

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

There are multiple vulnerabilities in Java™ Technology Edition used by the Elastic Storage Server. Fixes for all these vulnerabilities are available.

Vulnerability Details

CVEID: CVE-2023-22045 - An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause low confidentiality impacts.

CVEID: 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.

CVEID: CVE-2023-21967 - 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.

CVEID: CVE-2023-21954 - 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.

CVEID: 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.

CVEID: 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.

CVEID: 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.

CVEID: 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.

CVEID: 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 Elastic Storage Server/Systems	6.1.0.0 - 6.1.2.7
IBM Elastic Storage Server/Systems	6.1.3.0 - 6.1.8.3

Storage Scale Server
Storage Scale Systems

ESS Software:

- **Downloads and drivers:**
  - SCALE_SYSTEM_VM-6.1.9.0-x86_64-BYOE-EMS
  - Scale_System_DME_UNIFIED-6.1.9.0-ppc64LE-EMS
  - Scale_System_DAE_UNIFIED-6.1.9.0-ppc64LE-EMS
  - Scale_System_DME_UNIFIED-6.1.9.0-x86_64-EMS
  - Scale_System_DAE_UNIFIED-6.1.9.0-x86_64-EMS
- **Fixes:**
  - ESS_DME_BASEIMAGE_3200-6.1.2.8-x86_64-Linux
  - ESS_DAE_BASEIMAGE_3200-6.1.2.8-x86_64-Linux
  - ESS_DAE_BASEIMAGE_Legacy-6.1.2.8-ppc64LE-Linux
  - ESS_DME_BASEIMAGE_5000-6.1.2.8-ppc64LE-Linux
  - ESS_DAE_BASEIMAGE_3000-6.1.2.8-x86_64-Linux
  - ESS_DME_BASEIMAGE_Legacy-6.1.2.8-ppc64LE-Linux
  - ESS_DAE_BASEIMAGE_5000-6.1.2.8-ppc64LE-Linux
  - ESS_EMS_VM_6.1.9.0_has_been_rebranded_to_Storage_Scale_System_EMS_VM_6.1.9.0
  - ESS_DME_6.1.9.0_has_been_rebranded_to_Storage_Scale_System_DME_6.1.9.0
  - ESS_Firmware_6.1.9.0_has_been_rebranded_to_Storage_Scale_System_Firmware_6.1.9.0
  - ESS_DME_BASEIMAGE_3000-6.1.2.8-x86_64-Linux

- **IBM Storage Scale Software Version Recommendation Preventive Service Planning**

  IBM Storage Scale Software Version Recommendation
  Downloads and drivers:
  - ESS_DAE_6.1.9.0_has_been_rebranded_to_Storage_Scale_System_DAE_6.1.9.0

  Problem solving information
  - SMS hangs when trying to display a list of bootable devices

  Software:
  - Scale_System_VM-6.1.9.0-x86_64-UTILITY-EMS

Keep safe and a magnificent ‘24
Red, Belisama