Belisama

December Newsletter

Subscribe/Unsubscribe

Greetings all,
I hope that you manage to have a bit of a break before launching into an exciting ‘26. Looking back it has been an interesting year – We have seen that Power now goes all the way to 11 (and quite a different side to Bill Starke), AIX (or AI(x) as I would like to re-brand it) continues to offer new innovations – as does IBM I. We had a very success TechXChange in Florida and the IBM Champion community continues to grow in members and activities (Thanks Libby!).
Looking forward to working with you over the next year – Happy ‘26!

A few updates to share

- New to NIM, or experiencing issues? Andrey has a number of recent blogs:
  - NIM Overview
  - Issues with AIX TL4
- Which is timely as I have been playing with YubiKey / PowerSC MFA and AIX. I was about to publish, but as Andrey noted, AIX 7.3 TL4 has improved AIX SSH Security with FIDO2 Keys, which allows MFA using YubiKey. Will publish my testing results early next year.
  Old references for your background: AIX and PowerSC

Quick bites

New AIX and Availability Enhancements
Rob McNelly shares recent IBM news and notifications, including virtualization enhancements and security alerts
Link

Newsletter #31 2025-12-02
Mike Davidson newsletter has many useful links – and not only IBM i focused!
Link

Mastering AIX Migrations
Thanks Chris and the AIX Education team – a great new course “Mastering AIX Migrations”, which will teach you to:
By the end of this course, students will be able to:

- Describe AIX migration process requirements
- Explain the different methods available for migrating to a newer version of AIX

- Apply best practices for migrating and upgrading AIX
- Perform a migration to AIX 7.3 using AIX installation media
- Perform a migration to AIX 7.3 using NIM
- Perform a migration to AIX 7.3 using NIMADM

Community post
Course details
Badge

How Modern Malware Is Reaching IBM i, AIX, and Linux - Pro Tips for Protecting Your Systems
A session prepared by Fortra on Tech Channel
Malware and ransomware can devastate any system, including Power servers running IBM i, AIX, or Linux. Security by obscurity isn't cutting it anymore, but protecting your servers is simpler than you might think.
In this episode of Ask the Experts, Fortra's Sandi Moore and Mike Davison join host Tom Huntington to share their insight into the ways malware affects Power servers and what you can do to protect your systems.
Link

Coming soon

- **2026 and TechXChange!**

Redbooks and Redpapers

- **Security and Cyber Resilience with Power11**, Draft Redbook, 17 December 2025
  Link
- **IBM Storage Scale: Block Storage and High Performance File Access**, Redpaper, 16 December 2025
  Link

IBM alerts and notices

AIX PowerVM alerts:

- **AIX/VIOS is vulnerable to an out-of-bounds read (CVE-2025,9230, CVE-2025-9232) due to OpenSSL**
  Vulnerabilities in OpenSSL could allow an attacker to trigger an out-of-bounds read (CVE-2025-9230, CVE-2025-9232). OpenSSL is used by AIX as part of AIX's secure network communications.
  Vulnerability Details
  CVE-2025-9230 - Issue summary: An application trying to decrypt CMS messages encrypted using password based encryption can trigger an out-of-bounds read and write. Impact summary: This out-of-bounds read may trigger a crash which leads to Denial of Service for an application. The out-of-

bounds write can cause a memory corruption which can have various consequences including a Denial of Service or Execution of attacker-supplied code. Although the consequences of a successful exploit of this vulnerability could be severe, the probability that the attacker would be able to perform it is low. Besides, password based (PWRI) encryption support in CMS messages is very rarely used. For that reason the issue was assessed as Moderate severity according to our Security Policy. The FIPS modules in 3.5, 3.4, 3.3, 3.2, 3.1 and 3.0 are not affected by this issue, as the CMS implementation is outside the OpenSSL FIPS module boundary.
CVE-2025-9232 - Issue summary: An application using the OpenSSL HTTP client API functions may trigger an out-of-bounds read if the 'no_proxy' environment variable is set and the host portion of the authority component of the HTTP URL is an IPv6 address. Impact summary: An out-of-bounds read can trigger a crash which leads to Denial of Service for an application. The OpenSSL HTTP client API functions can be used directly by applications but they are also used by the OCSP client functions and CMP (Certificate Management Protocol) client implementation in OpenSSL. However the URLs used by these implementations are unlikely to be controlled by an attacker. In this vulnerable code the out of bounds read can only trigger a crash. Furthermore the vulnerability requires an attacker-controlled URL to be passed from an application to the OpenSSL function and the user has to have a 'no_proxy' environment variable set. For the aforementioned reasons the issue was assessed as Low severity. The vulnerable code was introduced in the following patch releases: 3.0.16, 3.1.8, 3.2.4, 3.3.3, 3.4.0 and 3.5.0. The FIPS modules in 3.5, 3.4, 3.3, 3.2, 3.1 and 3.0 are not affected by this issue, as the HTTP client implementation is outside the OpenSSL FIPS module boundary.

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
openssl.base	3.0.0.0	3.0.16.1000

Link

AIX alerts:

- **AIX is vulnerable to a denial of service (CVE-2025-9086) due to cURL libcurl**
  Vulnerability in cURL libcurl could allow a remote attacker to cause a denial of service (CVE-2025-9086). AIX uses cURL libcurl as part of rsyslog, LV/PV encryption integration with HPCS and in Live Update for interacting with HMC.
  CVE-2025-9086

1. A cookie is set using the `secure` keyword for `https://target`
2. curl is redirected to or otherwise made to speak with `http://target` (same hostname, but using clear text HTTP) using the same cookie set
3. The same cookie name is set - but with just a slash as path (`path='/'`). Since this site is not secure, the cookie *should* just be ignored.
4. A bug in the path comparison logic makes curl read outside a heap buffer boundary The bug either causes a crash or it potentially makes the comparison come to the wrong conclusion and lets the clear-text site override the contents of the secure cookie, contrary to expectations and depending on the memory contents immediately following the single-byte allocation that holds the path. The presumed and correct behaviour would be to plainly ignore the second set of the cookie since it was already set as secure on a secure host so overriding it on an insecure host should not be okay.

Affected Products and Versions

Affected Product(s)	Version(s)
AIX	7.3 TL1, 7.3 TL2, 7.3 TL3, 7.3 TL4

The following fileset levels are vulnerable:

Fileset	Lower Level	Upper Level
oss.lib.libcurl	7.79.1.0	7.79.1.0
oss.lib.libcurl	8.1.2.0	8.1.2.0
oss.lib.libcurl	8.5.0.0	8.5.0.2

Note: This bulletin does not apply to versions of curl installed from the AIX Toolbox.
Link

Firmware updates:

- **New Firmware New Microcode for Firmware 1050 .... for 1050.70**
  New "Informational" update for Power10 servers:
  - IBM Power E1050 (9043-MRX)
  - IBM Power L1022 (9786-22H)
  - IBM Power L1024 (9786-42H)
  - IBM Power S1014 (9105-41B)
  - IBM Power S1022 (9105-22A)
  - IBM Power S1022s (9105-22B)
  - IBM Power System E1080 Server (9080-HEX)

  Link

- **New Microcode for Firmware 950 .. 950.F1/950.G0**
  New "HIPER" update for Power9 servers:
  - Power System S914 (9009-41G)
  - Power System E950 Server (9040-MR9)
  - Power System E980 Server (9080-M9S)
  - Power System H922 Server (9223-22H)
  - Power System H922 Server (9223-22S)

- Power System H924 Server (9223-42H)
- Power System H924 Server (9223-42S)
- Power System L922 Server (9008-22L)
- Power System S914 Server (9009-41A)
- Power System S922 Server (9009-22A)
- Power System S922 Server (9009-22G)
- Power System S924 Server (9009-42A)
- Power System S924 Server (9009-42G)

Link

GPFS/Scale alerts:

- **The following vulnerabilities, which can affect IBM Storage Scale System could provide weaker-than-expected security, are now fixed in Storage Scale System 6.2.3.3 and 7.0.0.0 or higher (CVE-2024-50058, CVE-2024-46697, CVE-2024-43855, CVE-2024-42294, CVE-2024-36930, CVE-2024-42316, CVE-2024-42302, CVE-2024-41012, CVE-2024-41020, CVE-2024-26708, CVE-2024-26725, CVE-2024-42090, CVE-2024-26734, CVE-2024-26782, CVE-2024-26900, CVE-2024-4741, CVE-2024-2511).**
  Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale System	6.2.0.0 – 6.2.3.2

  Link

- **The following vulnerabilities that can affect IBM Storage Scale Management GUI are now addressed in 5.2.3.5 and 6.0.0.0 (CVE-2025-6493)**
  The following vulnerabilities, which may affect IBM Storage Scale when the Management GUI is configured and could lead to weaker-than-expected security, have been remediated in Storage Scale version 5.2.3.5 and later and 6.0.0.0 and later (CVE-2025-6493)
  Vulnerability Details
  CVE-2025-6493 - A weakness has been identified in CodeMirror up to 5.65.20. Affected is an unknown function of the file mode/markdown/markdown.js of the component Markdown Mode. This manipulation causes inefficient regular expression complexity. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be exploited. Upgrading to version 6.0 is able to address this issue. You should upgrade the affected component. Not all code samples mentioned in the GitHub issue can be found. The repository mentions, that "CodeMirror 6 exists, and is [...] much more actively maintained."
  Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale	5.2.3.0 - 5.2.3.4

  Link

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

  IBM strongly recommends at least an annual upgrade of Scale code to stay at the recommended or latest levels of code as defined in the tables below.

IBM Storage Scale	Minimum Level Note: Neither fixes nor root cause analysis will be provided for code level below minimum level	Recommended Level
IBM Storage Scale 6.0.0.x Stream	6.0.0.0 (Oct 2025)	6.0.0.0 (Oct 2025)
IBM Storage Scale(EUS stream 5.2.3.x)	5.2.3.3[August 2025]	5.2.3.3[August 2025]
IBM Storage Scale 5.2.x stream	5.2.0.1[June 2024]	5.2.2.1[Feb 2025]
IBM Storage Scale (priorEUS stream 5.1.9.x)	5.1.9.12[Sep2025]	5.1.9.12[Sep2025]

Note: 5.1.x End of Service on Sept. 30, 2025

IBM Storage Scale System	Minimum Level Note: Neither fixes nor root cause analysis will be provided for code level below minimum level	Recommended Level	Latest Level
IBM Storage Scale System 3000, 3200, 3500, 5000, and 6000 5.2.x Stream	ESS 6.2.1.0[Aug 2024]	ESS 6.2.2.1[Mar 2025]	ESS 6.2.3.2 [Sep2025]
IBM Storage Scale System 3000, 3200, 3500, 50005.1.x stream Read the top of this page about 5.1.x End of Service on Sept. 30, 2025	ESS 6.1.9.8[Oct 2025]	ESS 6.1.9.8[Oct 2025]	ESS 6.1.9.8[Oct 2025]

Containerised Storage Scale1,2	Minimum Level Note: Neither fixes nor root cause analysis will be provided for code level below minimum level	Recommended Level	Latest Level
IBM Storage Scale Container Native Storage Access (CNSA)	6.0.0 stream: 6.0.0.0[Oct 2025]	6.0.0 stream: 6.0.0.0[Oct 2025]	6.0.0 stream: 6.0.0.1[Dec 2025]
	5.2.x stream: 5.2.0.1[Jun 2024]	5.2.3 stream: 5.2.3.5[Nov 2025]	5.2.3 stream: 5.2.3.5[Nov 2025]
IBM Storage Scale Container Storage Interface (CSI) (stand-alone)	3.0.x stream: 3.0.0[Oct 2025]	3.0.x stream: 3.0.0[Oct2025]	3.0.x stream: 3.0.1[Dec 2025]
	2.y.x stream: 2.11.1[Jun 2024]	2.14.x stream: 2.14.4[Nov2025]	2.14.x stream: 2.14.4[Nov 2025]

Link

Keep safe and best wishes for a calmer ‘26!
Red, Belisama