Belisama

August Newsletter

Subscribe/Unsubscribe

Greetings all,
I trust that you have all seen the latest set of fixes that IBM has released as there have been critical fixes for AIX, PowerVM and the HMC (HMC). The latest fixes for AIX and PowerVM are available on supported levels. I have included further details below.

A few updates to share

- If you are interested in monitoring your Power environment, have a look at Andrey's Blog outlining his use of Prometheus, Grafana and Alertmanager. I have used Grafana in the past to display data sent from systems, but Andrey has put together a comprehensive solution.
  Link

Quick bites

Moving from Logical Units Shared Storage Pools (SSP)
Support has put together a document describing the steps involved in moving existing LUs from one Shared Storage Pool (SSP) to New SSP cluster or same SSP cluster.
Link

In case you missed ….

- **PowerVUG: Evaluating SAN IO to-from Memory with Earl Jew and Eddie Garza**
  In this August Session, Earl Jew and Eddie Garza discusses what is often forgotten, how quickly memory receives SAN reads and stages SAN writes. Supporting SAN I/O is becoming a critical factor in managing performance.
  Session Replay
  Slides

Redbooks and Redpapers

- **IBM Storage Scale Container Native: Implementation Guide for Kubernetes and Red Hat OpenShift**, Redbook, published 21 August 2026 , Redpaper, revised: August 4, 2022
  Link
- **IBM Power S1112 Technical Overview and Introduction**, Redbook, published 27 August, 2026
  Link
- **Modernising IBM i Applications**, Redbook, published 12 August 2026
  Link

- **The Definitive Guide to IBM Storage FlashSystem and AIX Integration**, Redbook, published 04 August 2026
  Link

IBM alerts and notices

AIX Hiper:

- **APAR IJ57855 Some FC adapters may not recover from temporary SAN errors**

Affected Domain

AIX 7.2 TL05
AIX 7.3 TL04 / TL03 / TL02
VIOS 4.1.2 / 4.1.1 / 4.1.0

Description

UPDATE August 21, 2026 - The fixing levels for AIX7.3TL02 and VIOS 4.1.0 in the "Affected AIX/VIOS Levels..." table have been updated to AIX 7300-02-05 and VIOS 4.1.0.50, respectively. The rest of the bulletin, originally published on July 23, 2006, remains unchanged.
Certain fibre channel adapters may not recover from SAN errors that would normally cause only temporary link down events.
Affected adapters include any that use the cvfcdd driver. Identify if these adapters are in use by the VIOS or AIX partition by running the following as root:

lsdev -c adapter | grep fcs | grep 7710

or

odmget -q ddins=pci/cvfcdd CuDv

This issue can occur when SFP monitoring or 'fcstat -e' command is executed before a link transition (link up or link down). As a result, environments that regularly run 'fcstat -e' to collect adapter statistics are at higher risk of encountering the problem. Once triggered, the adapter remains in a link-down state and recovery may require an LPAR reboot.
As a temporary workaround until the corrective fix is applied, avoid running '*fcstat -e*' and SFP-monitoring utilities on systems equipped with affected adapters.

Affected AIX/VIOS Levels

AIX 7300-04
AIX 7300-04-01
AIX 7300-03
AIX 7300-03-02-2546
AIX 7300-03-03
AIX 7300-02
AIX 7300-02-04-2520
AIX 7300-02-05
AIX 7200-05
AIX 7200-05-11-2546

AIX 7200-05-12
VIOS 4.1.2.0
VIOS 4.1.2.10
VIOS 4.1.1.0
VIOS 4.1.1.20
VIOS 4.1.1.30
VIOS 4.1.0.0
VIOS 4.1.0.40
VIOS 4.1.0.50

Link

- **RMC daemon (part of Reliable Scalable Cluster Technology) is vulnerable to Denial-of-Service attack**
  RMC daemon (part of Reliable Scalable Cluster Technology) is vulnerable for Denial-of-Service attack while handling malformed packets during a RMCAPI session establishement.
  Vulnerability Details
  CVE-2026-14514 - IBM Reliable Scalable Cluster Technology (RSCT) 3.0 could allow a remote attacker to cause a denial of service by sending a specially crafted request due improper input validation.
  Affected Products and Versions

Affected Product(s)	Version(s)
RSCT	3.3
RSCT	3.2

  The vulnerabilities in the following filesets are being addressed:

Fileset	Lower Level	Upper Level
rsct.core.rmc	3.3.4.0	3.3.4.2
rsct.core.rmc	3.3.3.0	3.3.3.2
rsct.core.rmc	3.3.2.0	3.3.2.2
rsct.core.rmc	3.2.6.0	3.2.6.6

  Link

- **Vulnerabilities in IBM AIX and PowerVM VIOS**
  Updated Aug 21, 2026: Updated the summary to highlight the additional installation instructions. IBM is providing security updates for supported AIX and VIOS releases that are under active fix support. Delivered through Service Packs (SPs) and Fix Packs (FPs), these updates remediate vulnerabilities affecting operating system, virtualisation, and third-party components as described in the vulnerability details section. To simplify deployment and maintenance, the security fixes have been incorporated into cumulative maintenance packages. IBM strongly recommends that customers remain on supported releases and promptly apply all applicable security updates and fixes. Please review the Remediation/Fixes and Release Notes sections

before deployment. Special steps are required while using NIM to apply the updates. Additional steps are also required after applying VIOS 4.1.0/4.1.1 updates.
Affected Products and Versions

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

The vulnerabilities in the following filesets are being addressed:
key_fileset = aix

Fileset	Lower Level	Upper Level	KEY
bos.mp64	7.2.5.0	7.2.5.212	key_w_fs
bos.mp64	7.3.2.0	7.3.2.5	key_w_fs
bos.mp64	7.3.3.0	7.3.3.2	key_w_fs
bos.mp64	7.3.4.0	7.3.4.1	key_w_fs

IBM has assigned the following APARs to this problem:

AIX Level	APAR	Availability	SP	KEY
7.2.5	IJ59566	08/14/2026	SP13	key_w_apar
7.3.2	IJ59565	08/14/2026	SP05	key_w_apar
7.3.3	IJ59564	08/14/2026	SP03	key_w_apar
7.3.4	IJ59563	08/14/2026	SP02	key_w_apar

VIOS Level	APAR	Availability	SP	KEY
4.1.0	IJ59565	08/14/2026	4.1.0.50	key_w_apar
4.1.1	IJ59564	08/14/2026	4.1.1.30	key_w_apar
4.1.2	IJ59563	08/14/2026	4.1.2.20	key_w_apar

IBM strongly recommends addressing the vulnerability now.

AIX Level	Service Pack
AIX 7.3 TL04	SP2
AIX 7.3 TL03	SP3
AIX 7.3 TL02	SP5
AIX 7.2 TL05	SP13

PowerVM VIOS Level	Fix Pack
VIOS 4.1.2	4.1.2.20
VIOS 4.1.1	4.1.1.30
VIOS 4.1.0	4.1.0.50

Link

Power Firmware (HIPER):

- **Power10 firmware**
  The latest service pack 1060.81 is now available for system firmware levels, ML1060, MM1060 and MH1060.
  This service pack resolves the following issues:
  IMPORTANT NOTE: Some of these issues are deferred fixes such that the security issue is not fully mitigated until a re-ipl of the system has been completed

The following fixes are being released to mitigate management network attacks against the service processor:

A security problem was fixed for CVE-2026-16687
A security problem was fixed for CVE-2026-16835
A security problem was fixed for CVE-2026-16832
A security problem was fixed for CVE-2026-18848
A security problem was fixed for CVE-2026-16828
A security problem was fixed for CVE-2026-18681
A security problem was fixed for CVE-2026-16724
A security problem was fixed for CVE-2026-18849

The following fixes are being released to mitigate service processor attacks against the host:

A security problem was fixed for CVE-2026-16938
A security problem was fixed for CVE-2026-16933
A security problem was fixed for CVE-2026-18871
A security problem was fixed for CVE-2026-16930
A security problem was fixed for CVE-2026-17429
A security problem was fixed for CVE-2026-17063
A security problem was fixed for CVE-2026-16707
A security problem was fixed for CVE-2026-17100
A security problem was fixed for CVE-2026-16661
A security problem was fixed for CVE-2026-17093
A security problem was fixed for CVE-2026-19234
A security problem was fixed for CVE-2026-19321

The following fixes are being released to mitigate host network attacks against a partition:

A security problem was fixed for CVE-2026-18821
A security problem was fixed for CVE-2026-17028
A security problem was fixed for CVE-2026-17414

The following fixes are being released to mitigate a guest partition attacking the host firmware/hypervisor:

A security problem was fixed for CVE-2026-17091
A security problem was fixed for CVE-2026-17097

Others:

A security problem was fixed for CVE-2026-4936. A re-IPL of the system is required for the security fix to take effect.
A security problem was fixed for CVE-2026-4937. The corresponding security bulletin includes additional details on how to complete the mitigation.
A security problem was fixed for CVE-2026-15961.
A security problem was fixed for CVE-2026-45447
A security problem was fixed for CVE-2026-52943, CVE-2026-43373, CVE-2026-43194

Link

- **Power9 firmware (HIPER)**
  The latest service pack 950.H3 is now available for system firmware levels VL950, VM950, and VH950.
  This service pack addresses the following issues:
  IMPORTANT NOTE: Some of these issues are deferred fixes such that the security issue is not fully mitigated until a re-ipl of the system has been completed
  The following fixes are being released to mitigate management network attacks against the service processor:
  A security problem was fixed for CVE-2026-16687
  A security problem was fixed for CVE-2026-16835
  A security problem was fixed for CVE-2026-16832
  A security problem was fixed for CVE-2026-18848
  A security problem was fixed for CVE-2026-16828
  A security problem was fixed for CVE-2026-18681
  The following fixes are being released to mitigate service processor attacks against the host:
  A security problem was fixed for CVE-2026-16938
  A security problem was fixed for CVE-2026-16933
  A security problem was fixed for CVE-2026-17429
  A security problem was fixed for CVE-2026-16707
  A security problem was fixed for CVE-2026-17100
  A security problem was fixed for CVE-2026-16661
  A security problem was fixed for CVE-2026-17093
  The following fixes are being released to mitigate host network attacks against a partition:
  A security problem was fixed for CVE-2026-18821
  A security problem was fixed for CVE-2026-17028
  A security problem was fixed for CVE-2026-17414
  The following fixes are being released to mitigate a guest partition attacking the host firmware/hypervisor:
  A security problem was fixed for CVE-2026-17042
  A security problem was fixed for CVE-2026-17091
  A security problem was fixed for CVE-2026-17097
  Others:
  A security problem was fixed for CVE-2026-4936. A re-IPL of the system is required for the security fix to take effect.
  A security problem was fixed for CVE-2026-4937. The corresponding security bulletin includes additional details on how to complete the mitigation.
  A security problem was fixed for CVE-2026-45447
  A security problem was fixed for CVE-2026-52943, CVE-2026-43373, CVE-2026-43194

Link

PowerVM:

- **Unauthenticated Access to CGI Scripts Protected by Directory Rules via script_alias in Erlang OTP (inets modules)**
  Incorrect Authorisation vulnerability in Erlang OTP (inets modules) allows unauthenticated access to CGI scripts protected by directory rules when served via script_alias. When script_alias maps a URL prefix to a directory outside DocumentRoot, mod_auth evaluates directory-based access controls against the DocumentRoot-relative path while mod_cgi executes the script at the ScriptAlias-resolved path. This path mismatch allows unauthenticated access to CGI scripts that directory rules were meant to protect. This vulnerability is associated with program files lib/inets/src/http_server/mod_alias.erl, lib/inets/src/http_server/mod_auth.erl, and lib/inets/src/http_server/mod_cgi.erl. This issue affects OTP from OTP 17.0 before OTP 28.4.2, OTP 27.3.4.10 and OTP 26.2.5.19, corresponding to inets from 5.10 before 9.6.2, 9.3.2.4 and 9.1.0.6.
  Vulnerability Details
    CVE-2026-28808 - Incorrect Authorisation vulnerability in Erlang OTP (inets modules) allows unauthenticated access to CGI scripts protected by directory rules when served via script_alias. When script_alias maps a URL prefix to a directory outside DocumentRoot, mod_auth evaluates directory-based access controls against the DocumentRoot-relative path while mod_cgi executes the script at the ScriptAlias-resolved path. This path mismatch allows unauthenticated access to CGI scripts that directory rules were meant to protect. This vulnerability is associated with program files lib/inets/src/http_server/mod_alias.erl, lib/inets/src/http_server/mod_auth.erl, and lib/inets/src/http_server/mod_cgi.erl. This issue affects OTP from OTP 17.0 before OTP 28.4.2, OTP 27.3.4.10 and OTP 26.2.5.19, corresponding to inets from 5.10 before 9.6.2, 9.3.2.4 and 9.1.0.6.
  Affected Products and Versions

Affected Product(s)	Version(s)
PowerVC	2.3.1, 2.3.2, 2.3.3

  Link
- PowerVM fixes:

Issue	Fix
Mako Template Lookup Path Traversal Vulnerability Fixed in 1.3.11	Link
Improper Chain of Trust in Erlang OTP's pubkey_cert Module Allows Certificate Forgery	Link
Predictable Numbers/Identifiers Vulnerability in Erlang/OTP Kernel inet_res & inet_db Modules: DNS Cache Poisoning Risk	Link
i18nextify JavaScript Library: URL-Injection Vulnerability Prior to 3.0.5	Link

Axios Prototype Pollution Vulnerability Fixed in Version 1.15.2	Link
Axios Prototype Pollution: Intercept JSON Responses or Hijack HTTP Transport	Link
Axios Prototype Pollution Vulnerability: Object.prototype Pollution Leading to Privilege Escalation and Authorization Bypass in Axios Library Prior to 1.15.2	Link
IP-Address Library Vulnerability: XSS Risk with Untrusted Input Rendering and HTML Escaping Issues	Link
Erlang OTP SSH Path Traversal Vulnerability Affects File Attribute Modification and Privilege Escalation	Link
Pillow Integer Overflow Vulnerability Fixed in Version 12.2.0	Link
QS.stringify TypeError with arrayFormat: comma and encodeValuesOnly:true on null/undefined Arrays	Link
IDNA for Python Vulnerability: Resource Consumption and Denial-of-Service Risk with Long Inputs	Link
UltraJSON Memory Leak Fix in ujson.dump() Prior to 5.12.1	Link
Cross-Origin Redirect Headers Vulnerability in urllib3 Prior to 2.7.0	Link
Mako Template Library Vulnerability: Backslash Traversal on Windows Prior to Version 1.3.12	Link
Catastrophic Backtracking Vulnerability in path-to-regexp with Three or More Parameters	Link
lxml Local File Access Vulnerability: Fixed in 6.1.0	Link
DNS Name Constraints Validation Issue Fixed in cryptography v46.0.6	Link
Pallets Click 8.3.2 Command Injection Vulnerability	Link

GPFS / Scale fixes:

- **The following vulnerabilities that can affect IBM Storage Scale and the Samba Cluster Export Services (CES) layer are now addressed in 6.0.1.1 or higher**
  The following vulnerabilities, which can affect IBM Storage Scale and the Samba Cluster Export Services (CES) layer and could provide weaker-than-expected security, are now addressed in Storage Scale 6.0.1.1 or higher. CVE-2026-4408.
  Vulnerability Details
  CVE-2026-4408 - A flaw was found in Samba. A remote attacker can exploit a misconfiguration in Samba file servers and classic domain controllers that use the "check password script" feature. If this script is configured with the %u substitution character, the client-controlled username is passed without proper escaping of shell meta-characters. This vulnerability allows an attacker to achieve remote command execution on the affected system. This issue primarily affects non-standard configurations where the "check password script" is used with %u and the samba-dcerpcd service is started as a system service.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale	6.0.0.0 - 6.0.1.0

Link

- **IBM Storage Scale 6.0.1.0 - 6.0.1.1 and IBM Storage Scale System 7.0.1.0: File systems with DMAPI fail to mount on remote cluster nodes**

With versions 6.0.1.0 through 6.0.1.1 of IBM Storage Scale, mounting file systems that have DMAPI enabled fails on remote cluster nodes.

Content

When a file system has DMAPI enabled, the mmlsfs <file_system_name> -z command shows yes as:

```
# /usr/lpp/mmfs/bin/mmlsfs fs1 -z
flag        value          description
------------------- ------------------------ ----------------------------------
-z yes Is DMAPI enabled?
```

If you try to mount this file system on a remote cluster, the mount fails and the mount command returns an error.

Users Affected

Users that run IBM Storage Scale 6.0.1.0 or 6.0.1.1 on a storage cluster where the storage cluster has a DMAPI-enabled file system and that file system attempts to be mounted on remote cluster nodes. IBM Storage Scale System 7.0.1.0 is affected by this issue, too.

Problem Determination

The mount command on the remote cluster node fails with an error similar to the following example.

```
# /usr/lpp/mmfs/bin/mmmount /gpfs/fs1
Tue Aug 11 01:43:07 PM PDT 2026: mmmount: Mounting file systems ...
mount: /gpfs/fs1: cannot mount fs1 read-only.
mmmount: Command failed. Examine previous error messages to determine cause.
```

The mmfs.log on the client node reports a mount error. Note the "return code 13" and "err 13" in the next output:

```
2026-08-11_13:42:43.098-0700: [I] Command: mount fs1
2026-08-11_13:42:44.412-0700: [X] File System fs1 unmounted by the system with return code 13, reason code 0, at line 2643 in /project/sprelgpfs601/build/rgpfs6012623a/src/avs/fs/mmfs/ts/fs/mount.C
2026-08-11_13:42:44.412-0700: Permission denied
2026-08-11_13:42:44.412-0700: [W] Command: err 13: mount fs1
2026-08-11_13:42:44.412-0700: Permission denied
```

And the cluster manager node in the storage cluster logs a rejected RPC call:

2026-08-11_13:43:09.277-0700: [W] Access denied due to failed multitenancy authorization: RPC service 000E0001, msg 'ccMsgDmGetAllSessions', msg_id 222, from 10.21.102.186 home cluster name: storage-cluster-node-1.local err 13.
2026-08-11_13:43:09.603-0700: [E] File system fs1 unmounted by node 10.21.102.186 (remote-cluster-node-1.local in remote-cluster.local

Recommendations

DMAPI enabled file systems owned by a 6.0.1.0 / 6.0.1.1 cluster necessitate a workaround or fix to be remotely mounted. We suggest using the workaround below; but an eFix for APAR IJ59616 may be requested if required. This advisory will be updated when a fix in a formal build is available.
As a workaround, the additional security introduced with IBM Storage Scale 6.0.1.0 can be disabled. To do this, run the next command in the affected storage cluster:
Note: This reduces the protection against attacks from untrusted remote clusters to the storage cluster back to level prior to 6.0.1.0.

echo 999 | mmchconfig mtsecCheckEnabled=0 -i

After the fix is installed, revert the configuration change to re-enable the security feature:

echo 999 | /usr/lpp/mmfs/bin/mmchconfig mtsecCheckEnabled=DELETE -i

Link

- **Potential for undetected data loss in pwritev2 system call (HIPER)**

Risk categories

Data Loss

Abstract

IBM Storage Scale does not correctly handle the RWF_APPEND, RWF_NOAPPEND, RWF_SYNC, and RWF_DSYNC flags in the pwritev2 system call of Linux, causing undetected data loss.

Description

In all Linux distributions currently supported with IBM Storage Scale, pwritev2 is an available system call that allows applications to specify the flags RWF_SYNC, RWF_DSYNC, RWF_APPEND and RWF_NOAPPEND. Other flags are out of scope of this discussion. IBM Storage Scale does not handle these flags and does not provide a notification back to the application about its incompatibility with these flags.
For the RWF_SYNC and RWF_DSYNC flag, the result with IBM Storage Scale is that the data is not immediately synced to disk, even though this is required by the semantics of these flags. The NFS server of the Linux kernel also uses these flags for stable NFS writes. Those writes are affected in the same way in that the data is not immediately synced to disk, even though stable NFS writes make that guarantee.

For the RWF_APPEND and RWF_NOAPPEND flags, IBM Storage Scale did not take action on those either, possibly resulting in data being placed in the wrong place in the file (e.g., in the middle of the file instead of at the end). Depending on the Linux distribution version, not all of these flags are available; for example, RHEL 8 does not include support for the RWF_NOAPPEND and RWF_APPEND flags, and RHEL 9 does not include support for the RWF_NOAPPEND flag. For the flags that are supported on each Linux distro, the described problems exist.

Users Affected

All versions of Scale running on Linux are affected. This affects applications using the pwritev2 system call with the RWF_SYNC, RWF_DSYNC, RWF_APPEND, and RWF_NOAPPEND flags, but the specific system calls that are used by applications is usually only known by the application owner. Further, the NFS server of the Linux kernel is affected by the missing support for the sync flags, which includes CNFS; the result is that stable NFS writes are not immediately synced to disk.

Problem Determination

There is no system notification of these problems. You must inspect the file data. If a node crashes immediately after completing a write by using the RWF_SYNC or RWF_DSYNC flags, or issuing NFS stable writes to the NFS server of the Linux kernel (including CNFS), the data can be lost. If you are using the RWF_APPEND or RWF_NOAPPEND flags, only inspecting the data would reveal whether the write has been misplaced.

Recommended Action

Request an interim fix (efix) for this problem (APAR IJ59613). This advisory will be updated when a fix in a formal build is available.

Link

- **The following vulnerabilities that can affect IBM Storage Scale and the HDFS layer are now addressed in 5.2.3.8 or higher and 6.0.1.1 or higher**

  The following vulnerabilities, which can affect IBM Storage Scale and the HDFS layer and could provide weaker-than-expected security, are now addressed in Storage Scale 5.2.3.8 or higher and 6.0.1.1 or higher. (CVE-2026-33558, CVE-2026-2332, CVE-2026-33870, CVE-2025-11143)

  Vulnerability Details

  CVE-2026-33558 - Information exposure vulnerability has been identified in Apache Kafka. The NetworkClient component will output entire requests and responses information in the DEBUG log level in the logs. By default, the log level is set to INFO level. If the DEBUG level is enabled, the sensitive information will be exposed via the requests and responses output log. The entire lists of impacted requests and responses are: * AlterConfigsRequest * AlterUserScramCredentialsRequest * ExpireDelegationTokenRequest * IncrementalAlterConfigsRequest * RenewDelegationTokenRequest * SaslAuthenticateRequest * createDelegationTokenResponse *

describeDelegationTokenResponse * SaslAuthenticateResponse This issue affects Apache Kafka: from any version supported the listed API above through v3.9.1, v4.0.0. We advise the Kafka users to upgrade to v3.9.2, v4.0.1, or later to avoid this vulnerability.
CVE-2026-2332 - In Eclipse Jetty, the HTTP/1.1 parser is vulnerable to request smuggling when chunk extensions are used, similar to the "funky chunks" techniques outlined here: * https://w4ke.info/2025/06/18/funky-chunks.html * https://w4ke.info/2025/10/29/funky-chunks-2.html Jetty terminates chunk extension parsing at \r\n inside quoted strings instead of treating this as an error. POST / HTTP/1.1 Host: localhost Transfer-Encoding: chunked 1;ext="val X 0 GET /smuggled HTTP/1.1 ... Note how the chunk extension does not close the double quotes, and it is able to inject a smuggled request.
CVE-2026-33870 - Netty is an asynchronous, event-driven network application framework. In versions prior to 4.1.132.Final and 4.2.10.Final, Netty incorrectly parses quoted strings in HTTP/1.1 chunked transfer encoding extension values, enabling request smuggling attacks. Versions 4.1.132.Final and 4.2.10.Final fix the issue.
CWE: CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
CVE-2025-11143 - The Jetty URI parser has some key differences to other common parsers when evaluating invalid or unusual URIs. Differential parsing of URIs in systems using multiple components may result in security by-pass. For example a component that enforces a black list may interpret the URIs differently from one that generates a response. At the very least, differential parsing may divulge implementation details.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale	5.2.3.0 - 5.2.3.7
IBM Storage Scale	6.0.0.0 - 6.0.1.0

Link

- **The following vulnerabilities that can affect IBM Storage Scale and the Management GUI are now fixed in 5.2.3.9 or higher and 6.0.1.1 or higher**
  The following vulnerabilities, which can affect IBM Storage Scale and the Management GUI and could provide weaker-than-expected security, are now fixed in Storage Scale 5.2.3.9 or higher and 6.0.1.1 or higher. (CVE-2026-19483, CVE-2026-13460)
  Vulnerability Details
  CVE-2026-19483 - Secrets may be disclosed in log files in IBM Storage Scale Management GUI The admin password is logged into the GUI log of IBM Storage Scale Systems Deploy and Upgrade from GUI. Secrets may be disclosed in information related to exceptions in IBM Storage Scale Management GUI.

CVE-2026-13460 - IBM Storage Scale GUI contains a hardcoded token in the source code, which was used for inter-node cluster communication and REST API authentication between GUI.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale	5.2.3.0 - 5.2.3.8
IBM Storage Scale	6.0.0.0 - 6.0.1.0

Link

- **The following vulnerabilities that can affect IBM Storage Scale System monitoring layer are now fixed in 5.2.3.9 or higher and 6.0.1.1 or higher**
  The following vulnerabilities, which can affect IBM Storage Scale System monitoring layer and could provide weaker-than-expected security, are now fixed in Storage Scale 5.2.3.9 or higher and 6.0.1.1 or higher
  Vulnerability Details
  CVE-2026-7246- Pallets Click, versions 8.3.2 and below, contain a command injection vulnerability in the click.edit() function, allowing attackers to pass arbitrary OS commands from an unprivileged account.
  CVE-2026-44431 - urllib3 is an HTTP client library for Python. From 1.23 to before 2.7.0, cross-origin redirects followed from the low-level API via ProxyManager.connection_from_url().urlopen(..., assert_same_host=False) still forward these sensitive headers. This vulnerability is fixed in 2.7.0.
  CVE-2026-44432 - urllib3 is an HTTP client library for Python. From 2.6.0 to before 2.7.0, urllib3 could decompress the whole response instead of the requested portion (1) during the second HTTPResponse.read(amt=N) call when the response was decompressed using the official Brotli library or (2) when HTTPResponse.drain_conn() was called after the response had been read and decompressed partially (compression algorithm did not matter here). These issues could cause urllib3 to fully decode a small amount of highly compressed data in a single operation. This could result in excessive resource consumption (high CPU usage and massive memory allocation for the decompressed data) on the client side. This vulnerability is fixed in 2.7.0.
  CVE-2026-9375 - urllib3 version 2.6.3 is vulnerable to a decompression bomb bypass in its streaming API (`preload_content=False`) when using Brotli support. The issue arises due to three independent code paths in `response.py` that bypass the `max_length` protection introduced in version 2.6.0 to mitigate CVE-2025-66471. Specifically, negative `max_length` values can be produced due to buffer arithmetic in `read()`, `flush_decoder` unconditionally overrides `max_length` to `-1`, and `_flush_decoder()` passes no limit at all, defaulting to unlimited decompression. This allows a malicious HTTP server to trigger an out-of-memory (OOM) condition by decompressing large payloads into memory, leading to a denial of service (DoS). The vulnerability affects urllib3 2.6.3 and Brotli 1.2.0 and impacts

applications and libraries using `requests` or `urllib3` to stream content from untrusted sources.
CVE-2026-45409 - Internationalised Domain Names in Applications (IDNA) for Python provides support for Internationalised Domain Names in Applications (IDNA) and Unicode IDNA Compatibility Processing. In versions prior to 3.15, payloads such as `'"\u0660" * N` or `'"\u30fb" * N + "\u6f22"` utilise the `valid_contexto` function prior to length rejection, and for high values of `N` will take a long time to process. This is the same issue as CVE-2024-3651, however the original remediation in 2024 was not a complete fix. A specially crafted argument to the `idna.encode()` function could consume significant resources. This may lead to a denial-of-service. Starting in version 3.14, the function rejects long inputs as soon as practicable prior to any further processing to minimise resource consumption. In version 3.15, this approach was extended to lesser used alternate functions (i.e. per-label conversions and codec support). A workaround is available. Domain names cannot exceed 253 characters in length. If this length limit is enforced prior to passing the domain to the `idna.encode()` function, it should no longer consume significant resources. This is triggered by arbitrarily large inputs that would not occur in normal usage, but may be passed to the library assuming there is no preliminary input validation by the higher-level application.

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Scale	IBM Storage Scale 5.2.0.0 - 5.2.3.8
IBM Storage Scale	IBM Storage Scale 6.0.0.0 - 6.0.1.0

Link

- **The following vulnerabilities that can affect IBM Storage Scale Cloud installation tool (cloudkit) are now fixed in 5.2.3.8 or higher and 6.0.1.1 or higher**

  The following vulnerabilities, which can affect IBM Storage Scale and the cloud deployment installation tool (cloudkit) could provide weaker-than-expected security, are now fixed in Storage Scale 5.2.3.8 or higher and 6.0.1.1.

  Vulnerability Details

  CVE-2026-29181 - OpenTelemetry-Go is the Go implementation of OpenTelemetry. From 1.36.0 to 1.40.0, multi-value baggage: header extraction parses each header field-value independently and aggregates members across values. This allows an attacker to amplify cpu and allocations by sending many baggage: header lines, even when each individual value is within the 8192-byte per-value parse limit. This vulnerability is fixed in 1.41.0.

  CWE: CWE-770: Allocation of Resources Without Limits or Throttling

  Affected Products and Versions

Affected Product(s)	Version(s)

IBM Storage Scale	IBM Storage Scale 5.2.0.0 - 5.2.3.7
IBM Storage Scale	IBM Storage Scale 6.0.0.0 - 6.0.1.0

Link

Keep safe and avoid the Pallet’s click vulnerability
Red, Belisama