



Security Bulletin: Additional security vulnerabilities are addressed with IBM Cloud Pak for Business Automation iFixes for April 2025.

Security Bulletin

Summary

In addition to vulnerabilities announced in Security Bulletin: Multiple security vulnerabilities are addressed with IBM Cloud Pak for Business Automation 24.0.0-IF005 and 24.0.1-IF002, the following security vulnerabilities are addressed with IBM Cloud Pak for Business Automation 24.0.0-IF005 and 24.0.1-IF002.

Vulnerability Details

CVEID: [CVE-2024-45310](https://www.cve.org/CVERecord?id=CVE-2024-45310) (<https://www.cve.org/CVERecord?id=CVE-2024-45310>)

DESCRIPTION: runc is a CLI tool for spawning and running containers according to the OCI specification. runc 1.1.13 and earlier, as well as 1.2.0-rc2 and earlier, can be tricked into creating empty files or directories in arbitrary locations in the host filesystem by sharing a volume between two containers and exploiting a race with `os.MkdirAll`. While this could be used to create empty files, existing files would not be truncated. An attacker must have the ability to start containers using some kind of custom volume configuration. Containers using user namespaces are still affected, but the scope of places an attacker can create inodes can be significantly reduced. Sufficiently strict LSM policies (SELinux/Apparmor) can also in principle block this attack -- we suspect the industry standard SELinux policy may restrict this attack's scope but the exact scope of protection hasn't been analysed. This is exploitable using runc directly as well as through Docker and Kubernetes. The issue is fixed in runc v1.1.14 and v1.2.0-rc3. Some workarounds are available. Using user namespaces restricts this attack fairly significantly such that the attacker can only create inodes in directories that the remapped root user/group has write access to. Unless the root user is remapped to an actual user on the host (such as with rootless containers that don't use `/etc/sub[ug]id`), this in practice means that an attacker would only be able to create inodes in world-writable directories. A strict enough SELinux or AppArmor policy could in principle also restrict the scope if a specific label is applied to the runc runtime, though neither the extent to which the standard existing policies block this attack nor what exact policies are needed to sufficiently restrict this attack have been thoroughly tested.

CWE: [CWE-61: UNIX Symbolic Link \(Symlink\) Following](https://cwe.mitre.org/data/definitions/61.html) (<https://cwe.mitre.org/data/definitions/61.html>)

CVSS Source: CVE.org

CVSS Base score: 3.6

CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N)

CVEID: [CVE-2024-9341](https://www.cve.org/CVERecord?id=CVE-2024-9341) (<https://www.cve.org/CVERecord?id=CVE-2024-9341>)

DESCRIPTION: Containers common could allow a remote authenticated attacker to bypass security

restrictions, caused by a flaw when FIPS mode is enabled in Go library. By using a specially crafted symbolic links, an attacker could exploit this vulnerability to bypass intended isolation between containers and the host system and gain access critical host files.

CWE: [CWE-59: Improper Link Resolution Before File Access \('Link Following'\)](#)

(<https://cwe.mitre.org/data/definitions/59.html>)

CVSS Source: Red Hat

CVSS Base score: 5.4

CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:L/A:N)

CVEID: [CVE-2025-1470](#) (<https://www.cve.org/CVERecord?id=CVE-2025-1470>)

DESCRIPTION: In Eclipse OMR, from the initial contribution to version 0.4.0, some OMR internal port library and utilities consumers of z/OS atoe functions do not check their return values for NULL memory pointers or for memory allocation failures. This can lead to NULL pointer dereference crashes. Beginning in version 0.5.0, internal OMR consumers of atoe functions handle NULL return values and memory allocation failures correctly.

CWE: [CWE-476: NULL Pointer Dereference](#) (<https://cwe.mitre.org/data/definitions/476.html>)

CVSS Source: NVD

CVSS Base score: 5.5

CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CVEID: [CVE-2025-1471](#) (<https://www.cve.org/CVERecord?id=CVE-2025-1471>)

DESCRIPTION: In Eclipse OMR versions 0.2.0 to 0.4.0, some of the z/OS atoe print functions use a constant length buffer for string conversion. If the input format string and arguments are larger than the buffer size then buffer overflow occurs. Beginning in version 0.5.0, the conversion buffers are sized correctly and checked appropriately to prevent buffer overflows.

CWE: [CWE-787: Out-of-bounds Write](#) (<https://cwe.mitre.org/data/definitions/787.html>)

CVSS Source: NVD

CVSS Base score: 7.8

CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVEID: [CVE-2024-21538](#) (<https://www.cve.org/CVERecord?id=CVE-2024-21538>)

DESCRIPTION: Versions of the package cross-spawn before 7.0.5 are vulnerable to Regular Expression Denial of Service (ReDoS) due to improper input sanitization. An attacker can increase the CPU usage and crash the program by crafting a very large and well crafted string.

CWE: [CWE-1333: Inefficient Regular Expression Complexity](#) (<https://cwe.mitre.org/data/definitions/1333.html>)

CVSS Source: CVE.org

CVSS Base score: 7.5

CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVEID: [CVE-2024-55565](#) (<https://www.cve.org/CVERecord?id=CVE-2024-55565>)

DESCRIPTION: nanoid (aka Nano ID) before 5.0.9 mishandles non-integer values. 3.3.8 is also a fixed

version.

CWE: [CWE-835: Loop with Unreachable Exit Condition \('Infinite Loop'\)](https://cwe.mitre.org/data/definitions/835.html) (<https://cwe.mitre.org/data/definitions/835.html>)

CVSS Source: CISA ADP

CVSS Base score: 4.3

CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N)

CVEID: [CVE-2025-27789](https://www.cve.org/CVERecord?id=CVE-2025-27789) (<https://www.cve.org/CVERecord?id=CVE-2025-27789>)

DESCRIPTION: Babel is a compiler for writing next generation JavaScript. When using versions of Babel prior to 7.26.10 and 8.0.0-alpha.17 to compile regular expression named capturing groups, Babel will generate a polyfill for the ``.replace`` method that has quadratic complexity on some specific replacement pattern strings (i.e. the second argument passed to ``.replace``). Generated code is vulnerable if all the following conditions are true: Using Babel to compile regular expression named capturing groups, using the ``.replace`` method on a regular expression that contains named capturing groups, and the code using untrusted strings as the second argument of ``.replace``. This problem has been fixed in `@babel/helpers`` and `@babel/runtime`` 7.26.10 and 8.0.0-alpha.17. It's likely that individual users do not directly depend on `@babel/helpers``, and instead depend on `@babel/core`` (which itself depends on `@babel/helpers``). Upgrading to `@babel/core`` 7.26.10 is not required, but it guarantees use of a new enough `@babel/helpers`` version. Note that just updating Babel dependencies is not enough; one will also need to re-compile the code. No known workarounds are available.

CWE: [CWE-1333: Inefficient Regular Expression Complexity](https://cwe.mitre.org/data/definitions/1333.html) (<https://cwe.mitre.org/data/definitions/1333.html>)

CVSS Source: security-advisories@github.com

CVSS Base score: 6.2

CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVEID: [CVE-2025-1838](https://www.cve.org/CVERecord?id=CVE-2025-1838) (<https://www.cve.org/CVERecord?id=CVE-2025-1838>)

DESCRIPTION: IBM Business Automation Workflow Authoring allows an authenticated user to bypass client-side data validation in an authoring user interface which could cause a denial of service.

CWE: [CWE-602: Client-Side Enforcement of Server-Side Security](https://cwe.mitre.org/data/definitions/602.html) (<https://cwe.mitre.org/data/definitions/602.html>)

CVSS Source: IBM

CVSS Base score: 6.5

CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CVEID: [CVE-2024-57965](https://www.cve.org/CVERecord?id=CVE-2024-57965) (<https://www.cve.org/CVERecord?id=CVE-2024-57965>)

DESCRIPTION: In axios before 1.7.8, lib/helpers/isURLSameOrigin.js does not use a URL object when determining an origin, and has a potentially unwanted `setAttribute('href',href)` call. NOTE: some parties feel that the code change only addresses a warning message from a SAST tool and does not fix a vulnerability.

CWE: [CWE-346: Origin Validation Error](https://cwe.mitre.org/data/definitions/346.html) (<https://cwe.mitre.org/data/definitions/346.html>)

CVSS Source: cve@mitre.org

CVSS Base score: 0

CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:N)

CVEID: [CVE-2023-4218](https://www.cve.org/CVERecord?id=CVE-2023-4218) (<https://www.cve.org/CVERecord?id=CVE-2023-4218>)

DESCRIPTION: Eclipse IDE could allow a local authenticated attacker to obtain sensitive information, caused by improper handling of XML external entity (XXE) declarations. By persuading a victim to open specially crafted XML content, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.

CWE: [CWE-611: Improper Restriction of XML External Entity Reference](https://cwe.mitre.org/data/definitions/611.html) (<https://cwe.mitre.org/data/definitions/611.html>)

CVSS Source: IBM X-Force

CVSS Base score: 5

CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N)

CVEID: [CVE-2025-27152](https://www.cve.org/CVERecord?id=CVE-2025-27152) (<https://www.cve.org/CVERecord?id=CVE-2025-27152>)

DESCRIPTION: axios is a promise based HTTP client for the browser and node.js. The issue occurs when passing absolute URLs rather than protocol-relative URLs to axios. Even if baseURL is set, axios sends the request to the specified absolute URL, potentially causing SSRF and credential leakage. This issue impacts both server-side and client-side usage of axios. This issue is fixed in 1.8.2.

CWE: [CWE-918: Server-Side Request Forgery \(SSRF\)](https://cwe.mitre.org/data/definitions/918.html) (<https://cwe.mitre.org/data/definitions/918.html>)

CVSS Source: IBM

CVSS Base score: 7.5

CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVEID: [CVE-2024-31141](https://www.cve.org/CVERecord?id=CVE-2024-31141) (<https://www.cve.org/CVERecord?id=CVE-2024-31141>)

DESCRIPTION: Files or Directories Accessible to External Parties, Improper Privilege Management vulnerability in Apache Kafka Clients. Apache Kafka Clients accept configuration data for customizing behavior, and includes ConfigProvider plugins in order to manipulate these configurations. Apache Kafka also provides FileConfigProvider, DirectoryConfigProvider, and EnvVarConfigProvider implementations which include the ability to read from disk or environment variables. In applications where Apache Kafka Clients configurations can be specified by an untrusted party, attackers may use these ConfigProviders to read arbitrary contents of the disk and environment variables. In particular, this flaw may be used in Apache Kafka Connect to escalate from REST API access to filesystem/environment access, which may be undesirable in certain environments, including SaaS products. This issue affects Apache Kafka Clients: from 2.3.0 through 3.5.2, 3.6.2, 3.7.0. Users with affected applications are recommended to upgrade kafka-clients to version >=3.8.0, and set the JVM system property "org.apache.kafka.automatic.config.providers=none". Users of Kafka Connect with one of the listed ConfigProvider implementations specified in their worker config are also recommended to add appropriate "allowlist.pattern" and "allowed.paths" to restrict their operation to appropriate bounds. For users of Kafka Clients or Kafka Connect in environments that trust users with disk and environment variable access, it is not recommended to set the system property. For users of the Kafka Broker, Kafka MirrorMaker 2.0, Kafka Streams, and Kafka command-line tools, it is not recommended to set the system property.

CWE: [CWE-269: Improper Privilege Management](https://cwe.mitre.org/data/definitions/269.html) (<https://cwe.mitre.org/data/definitions/269.html>)

CVSS Source: IBM X-Force

CVSS Base score: 6.8

CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N)

CVEID: [CVE-2024-52046](https://www.cve.org/CVERecord?id=CVE-2024-52046) (https://www.cve.org/CVERecord?id=CVE-2024-52046)

DESCRIPTION: The ObjectSerializationDecoder in Apache MINA uses Java's native deserialization protocol to process incoming serialized data but lacks the necessary security checks and defenses. This vulnerability allows attackers to exploit the deserialization process by sending specially crafted malicious serialized data, potentially leading to remote code execution (RCE) attacks. This issue affects MINA core versions 2.0.X, 2.1.X and 2.2.X, and will be fixed by the releases 2.0.27, 2.1.10 and 2.2.4. It's also important to note that an application using MINA core library will only be affected if the IoBuffer#getObject() method is called, and this specific method is potentially called when adding a ProtocolCodecFilter instance using the ObjectSerializationCodecFactory class in the filter chain. If your application is specifically using those classes, you have to upgrade to the latest version of MINA core library. Upgrading will not be enough: you also need to explicitly allow the classes the decoder will accept in the ObjectSerializationDecoder instance, using one of the three new methods: /** * Accept class names where the supplied ClassNameMatcher matches for * deserialization, unless they are otherwise rejected. * * @param classNameMatcher the matcher to use */ public void accept(ClassNameMatcher classNameMatcher) /** * Accept class names that match the supplied pattern for * deserialization, unless they are otherwise rejected. * * @param pattern standard Java regexp */ public void accept(Pattern pattern) /** * Accept the wildcard specified classes for deserialization, * unless they are otherwise rejected. * * @param patterns Wildcard file name patterns as defined by * {@link org.apache.commons.io.FilenameUtils#wildcardMatch(String, String) FilenameUtils.wildcardMatch} */ public void accept(String... patterns) By default, the decoder will reject *all* classes that will be present in the incoming data. Note: The FtpServer, SSHd and Vysper sub-project are not affected by this issue.

CWE: [CWE-502: Deserialization of Untrusted Data](https://cwe.mitre.org/data/definitions/502.html) (https://cwe.mitre.org/data/definitions/502.html)

CVSS Source: NVD

CVSS Base score: 9.8

CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVEID: [CVE-2024-21235](https://www.cve.org/CVERecord?id=CVE-2024-21235) (https://www.cve.org/CVERecord?id=CVE-2024-21235)

DESCRIPTION: Vulnerability in Java SE (component: Hotspot). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to accessible data as well as unauthorized read access to a subset of accessible data.

CVSS Source: Oracle

CVSS Base score: 4.8

CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVEID: [CVE-2024-21217](https://www.cve.org/CVERecord?id=CVE-2024-21217) (https://www.cve.org/CVERecord?id=CVE-2024-21217)

DESCRIPTION: Vulnerability in Java SE (component: Serialization). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS).

CWE: [CWE-502: Deserialization of Untrusted Data](https://cwe.mitre.org/data/definitions/502.html) (https://cwe.mitre.org/data/definitions/502.html)

CVSS Source: Oracle

CVSS Base score: 3.7

CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

CVEID: [CVE-2024-21210](https://www.cve.org/CVERecord?id=CVE-2024-21210) (https://www.cve.org/CVERecord?id=CVE-2024-21210)

DESCRIPTION: Vulnerability in Java SE (component: Hotspot). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some accessible data.

CWE: [CWE-203: Observable Discrepancy](https://cwe.mitre.org/data/definitions/203.html) (https://cwe.mitre.org/data/definitions/203.html)

CVSS Source: Oracle

CVSS Base score: 3.7

CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVEID: [CVE-2024-21208](https://www.cve.org/CVERecord?id=CVE-2024-21208) (https://www.cve.org/CVERecord?id=CVE-2024-21208)

DESCRIPTION: Vulnerability in Java SE (component: Networking). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS).

CWE: [CWE-203: Observable Discrepancy](https://cwe.mitre.org/data/definitions/203.html) (https://cwe.mitre.org/data/definitions/203.html)

CVSS Source: Oracle

CVSS Base score: 3.7

CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

CVEID: [CVE-2024-10917](https://www.cve.org/CVERecord?id=CVE-2024-10917) (https://www.cve.org/CVERecord?id=CVE-2024-10917)

DESCRIPTION: In Eclipse OpenJ9 versions up to 0.47, the JNI function GetStringUTFLength may return an incorrect value which has wrapped around. From 0.48 the value is correct but may be truncated to include a smaller number of characters.

CWE: [CWE-190: Integer Overflow or Wraparound](https://cwe.mitre.org/data/definitions/190.html) (https://cwe.mitre.org/data/definitions/190.html)

CVSS Source: NVD

CVSS Base score: 5.3

CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

Affected Products and Versions

Affected Product(s)	Version(s)	Status
IBM Cloud Pak for Business Automation	V24.0.1 - V24.0.1-IF001	Affected
IBM Cloud Pak for Business Automation	V24.0.0 - V24.0.0-IF004	Affected
IBM Cloud Pak for Business Automation	earlier unsupported versions	Affected

Remediation/Fixes

Affected Product(s)	Version(s)	Remediation / Fix
IBM Cloud Pak for Business Automation	V24.0.1 - V24.0.1-IF001	Apply security fix 24.0.1-IF002 (https://www.ibm.com/support/pages/node/7184634)
IBM Cloud Pak for Business Automation	V24.0.0 - V24.0.1-IF004	Upgrade and apply security fix 24.0.0-IF005 (https://www.ibm.com/support/pages/node/7184784)
IBM Cloud Pak for Business Automation	earlier unsupported versions	Upgrade to 24.0.0-IF005 (https://www.ibm.com/support/pages/node/7184784) or 24.0.1-IF002 (https://www.ibm.com/support/pages/node/7184634)


Any open source library may be included in one or more sub-components of IBM Cloud Pak for Business Automation. Open source updates are not always synchronized across all components. The CVE in this bulletin are specifically addressed by

CVE ID	Component
CVE-2024-21538	Base Images
CVE-2025-27152	Business Automation Studio
CVE-2025-1470	Base Images
CVE-2025-1471	Base Images
CVE-2025-27152	Business Automation Workflow
CVE-2024-21235	Base Images
CVE-2024-21217	Base Images
CVE-2024-21210	Base Images
CVE-2024-21208	Base Images
CVE-2024-10917	Base Images
CVE-2024-45310	operators
CVE-2024-9341	operators
CVE-2023-4218	Business Automation Workflow
CVE-2024-57965	Business Automation Studio
CVE-2023-4218	Business Automation Workflow
CVE-2024-52046	Operational Decision Manager
CVE-2024-57965	Business Automation Workflow
CVE-2025-27789	Business Automation Workflow
CVE-2025-1838	Business Automation Studio
CVE-2025-27152	Business Automation Studio
CVE-2025-27789	Business Automation Studio
CVE-2024-57965	Business Automation Studio
CVE-2024-55565	Business Automation Studio
CVE-2024-31141	Operational Decision Manager

Workarounds and Mitigations

None

Get Notified about Future Security Bulletins

 Subscribe to [My Notifications](https://www.ibm.com/support/pages/node/718119) (<https://www.ibm.com/support/pages/node/718119>) to be notified of important product support alerts like this.

References

[Complete CVSS v3 Guide](#) 

[On-line Calculator v3](#) 

[Security Bulletin: Multiple security vulnerabilities are addressed with IBM Cloud Pak for Business Automation 24.0.0-IF005 and 24.0.1-IF002](#) (<https://www.ibm.com/support/pages/node/7232197>)

Related Information

[IBM Secure Engineering Web Portal](http://www.ibm.com/security/secure-engineering/bulletins.html) (<http://www.ibm.com/security/secure-engineering/bulletins.html>)

[IBM Product Security Incident Response Blog](http://www.ibm.com/blogs/psirt) (<http://www.ibm.com/blogs/psirt>)

Acknowledgement

Change History

03 May 2025: Initial Publication

*The CVSS Environment Score is customer environment specific and will ultimately impact the Overall CVSS Score. Customers can evaluate the impact of this vulnerability in their environments by accessing the links in the Reference section of this Security Bulletin.

Disclaimer

According to the Forum of Incident Response and Security Teams (FIRST), the Common Vulnerability Scoring System (CVSS) is an "industry open standard designed to convey vulnerability severity and help to determine urgency and priority of response." IBM PROVIDES THE CVSS SCORES ""AS IS"" WITHOUT WARRANTY OF ANY KIND, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY. In addition to other efforts to address potential vulnerabilities, IBM periodically updates the record of components contained in our product offerings. As part of that effort, if IBM identifies previously unidentified packages in a product/service inventory, we address relevant vulnerabilities regardless of CVE date. Inclusion of an older CVEID does not demonstrate that the referenced product has been used by IBM since that date, nor that IBM was aware of a vulnerability as of that date. We are making clients aware of relevant vulnerabilities as we become aware of them. "Affected Products and Versions" referenced in IBM Security Bulletins are intended to be only products and versions that are supported by IBM and have not passed their end-of-support or warranty date. Thus, failure to reference unsupported or extended-support products and versions in this Security Bulletin does not constitute a determination by IBM that they are

unaffected by the vulnerability. Reference to one or more unsupported versions in this Security Bulletin shall not create an obligation for IBM to provide fixes for any unsupported or extended-support products or versions.

Cross-reference information

Product	Component	Platform
+ IBM Cloud Pak for Automation		Platform Independent
+ IBM Cloud Pak for Business Automation		Platform Independent

Document Information

More support for:

[IBM Cloud Pak for Automation](https://www.ibm.com/mysupport/s/topic/0TO0z000000YgPmGAK) (https://www.ibm.com/mysupport/s/topic/0TO0z000000YgPmGAK)

Software version:

18.0.0, 18.0.1,18.0.2,19.0.1,19.0.2,19.0.3,20.0.1,20.0.2,20.0.3,21.0.1,21.0.2,21.0.3,22.0.1,22.0.2, 23.0.1, 23.0.2

Document number:

7232429

Modified date:

03 May 2025