Security Bulletin: Multiple Vulnerabilities in IBM Concert Software

Security Bulletin

Summary

Multiple vulnerabilities were addressed in IBM Concert Software version 2.3.1

Vulnerability Details

CVEID: CVE-2023-5752 *(https://www.cve.org/CVERecord?id=CVE-2023-5752)*
DESCRIPTION: When installing a package from a Mercurial VCS URL (ie "pip install hg+...") with pip prior to v23.3, the specified Mercurial revision could be used to inject arbitrary configuration options to the "hg clone" call (ie "--config"). Controlling the Mercurial configuration can modify how and which repository is installed. This vulnerability does not affect users who aren't installing from Mercurial.
CWE: CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') *(https://cwe.mitre.org/data/definitions/77.html)*
CVSS Source: Python Software Foundation
CVSS Base score: 5.5
CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N)

CVEID: CVE-2025-66400 *(https://www.cve.org/CVERecord?id=CVE-2025-66400)*
DESCRIPTION: mdast-util-to-hast is an mdast utility to transform to hast. From 13.0.0 to before 13.2.1, multiple (unprefixed) classnames could be added in markdown source by using character references. This could make rendered user supplied markdown code elements appear like the rest of the page. This vulnerability is fixed in 13.2.1.
CWE: CWE-20: Improper Input Validation *(https://cwe.mitre.org/data/definitions/20.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)

CVEID: CVE-2025-50181 *(https://www.cve.org/CVERecord?id=CVE-2025-50181)*
DESCRIPTION: urllib3 is a user-friendly HTTP client library for Python. Prior to 2.5.0, it is possible to disable redirects for all requests by instantiating a PoolManager and specifying retries in a way that disable redirects. By default, requests and botocore users are not affected. An application attempting to mitigate SSRF or open redirect vulnerabilities by disabling redirects at the PoolManager level will remain vulnerable. This issue has been patched in version 2.5.0.
CWE: CWE-601: URL Redirection to Untrusted Site ('Open Redirect') *(https://cwe.mitre.org/data/definitions/601.html)*
CVSS Source: NVD

CVSS Base score: 6.1

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

CVEID: CVE-2025-50182 *(https://www.cve.org/CVERecord?id=CVE-2025-50182)*

DESCRIPTION: urllib3 is a user-friendly HTTP client library for Python. Starting in version 2.2.0 and prior to 2.5.0, urllib3 does not control redirects in browsers and Node.js. urllib3 supports being used in a Pyodide runtime utilizing the JavaScript Fetch API or falling back on XMLHttpRequest. This means Python libraries can be used to make HTTP requests from a browser or Node.js. Additionally, urllib3 provides a mechanism to control redirects, but the retries and redirect parameters are ignored with Pyodide; the runtime itself determines redirect behavior. This issue has been patched in version 2.5.0.

CWE: CWE-601: URL Redirection to Untrusted Site ('Open Redirect') *(https://cwe.mitre.org/data/definitions/601.html)*

CVSS Source: NVD

CVSS Base score: 6.1

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

CVEID: CVE-2025-69873 *(https://www.cve.org/CVERecord?id=CVE-2025-69873)*

DESCRIPTION: ajv (Another JSON Schema Validator) before 8.18.0 is vulnerable to Regular Expression Denial of Service (ReDoS) when the $data option is enabled. The pattern keyword accepts runtime data via JSON Pointer syntax ($data reference), which is passed directly to the JavaScript RegExp() constructor without validation. An attacker can inject a malicious regex pattern (e.g., "^(a|a)*$") combined with crafted input to cause catastrophic backtracking. A 31-character payload causes approximately 44 seconds of CPU blocking, with each additional character doubling execution time. This enables complete denial of service with a single HTTP request against any API using ajv with $data: true for dynamic schema validation. This issue is also fixed in version 6.14.0.

CWE: CWE-1333: Inefficient Regular Expression Complexity *(https://cwe.mitre.org/data/definitions/1333.html)*

CVSS Source: cve@mitre.org

CVSS Base score: 2.9

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

CVEID: CVE-2025-54798 *(https://www.cve.org/CVERecord?id=CVE-2025-54798)*

DESCRIPTION: tmp is a temporary file and directory creator for node.js. In versions 0.2.3 and below, tmp is vulnerable to an arbitrary temporary file / directory write via symbolic link dir parameter. This is fixed in version 0.2.4.

CWE: CWE-59: Improper Link Resolution Before File Access ('Link Following') *(https://cwe.mitre.org/data/definitions/59.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)

CVEID: CVE-2025-61725 *(https://www.cve.org/CVERecord?id=CVE-2025-61725)*

DESCRIPTION: The ParseAddress function constructs domain-literal address components through repeated

string concatenation. When parsing large domain-literal components, this can cause excessive CPU consumption.

CVSS Source: CISA ADP

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-2025-67221 *(https://www.cve.org/CVERecord?id=CVE-2025-67221)*

DESCRIPTION: The orjson.dumps function in orjson thru 3.11.4 does not limit recursion for deeply nested JSON documents.

CWE: CWE-770: Allocation of Resources Without Limits or Throttling *(https://cwe.mitre.org/data/definitions/770.html)*

CVSS Source: CISA ADP

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-2025-13044 *(https://www.cve.org/CVERecord?id=CVE-2025-13044)*

DESCRIPTION: IBM Concert Software creates temporary files with predictable names, which allows local users to overwrite arbitrary files via a symlink attack.

CWE: CWE-340: Generation of Predictable Numbers or Identifiers *(https://cwe.mitre.org/data/definitions/340.html)*

CVSS Source: IBM

CVSS Base score: 6.2

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

CVEID: CVE-2025-5889 *(https://www.cve.org/CVERecord?id=CVE-2025-5889)*

DESCRIPTION: A vulnerability was found in juliangruber brace-expansion up to 1.1.11/2.0.1/3.0.0/4.0.0. It has been rated as problematic. Affected by this issue is the function expand of the file index.js. The manipulation leads to inefficient regular expression complexity. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. Upgrading to version 1.1.12, 2.0.2, 3.0.1 and 4.0.1 is able to address this issue. The name of the patch is a5b98a4f30d7813266b221435e1eaaf25a1b0ac5. It is recommended to upgrade the affected component.

CWE: CWE-400: Uncontrolled Resource Consumption *(https://cwe.mitre.org/data/definitions/400.html)*

CVSS Source: cna@vuldb.com

CVSS Base score: 3.1

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

CVEID: CVE-2026-21441 *(https://www.cve.org/CVERecord?id=CVE-2026-21441)*

DESCRIPTION: urllib3 is an HTTP client library for Python. urllib3's streaming API is designed for the efficient handling of large HTTP responses by reading the content in chunks, rather than loading the entire response body into memory at once. urllib3 can perform decoding or decompression based on the HTTP `Content-Encoding` header (e.g., `gzip`, `deflate`, `br`, or `zstd`). When using the streaming API, the library decompresses only the necessary bytes, enabling partial content consumption. Starting in version 1.22 and prior

to version 2.6.3, for HTTP redirect responses, the library would read the entire response body to drain the connection and decompress the content unnecessarily. This decompression occurred even before any read methods were called, and configured read limits did not restrict the amount of decompressed data. As a result, there was no safeguard against decompression bombs. A malicious server could exploit this to trigger excessive resource consumption on the client. Applications and libraries are affected when they stream content from untrusted sources by setting `preload_content=False` when they do not disable redirects. Users should upgrade to at least urllib3 v2.6.3, in which the library does not decode content of redirect responses when `preload_content=False`. If upgrading is not immediately possible, disable redirects by setting `redirect=False` for requests to untrusted source.

CWE: CWE-409: Improper Handling of Highly Compressed Data (Data Amplification) *(https://cwe.mitre.org/data/definitions/409.html)*

CVSS Source: NVD

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-2022-3248 *(https://www.cve.org/CVERecord?id=CVE-2022-3248)*

DESCRIPTION: A flaw was found in OpenShift API, as admission checks do not enforce "custom-host" permissions. This issue could allow an attacker to violate the boundaries, as permissions will not be applied.

CWE: CWE-863: Incorrect Authorization *(https://cwe.mitre.org/data/definitions/863.html)*

CVSS Source: IBM X-Force

CVSS Base score: 4.4

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

CVEID: CVE-2025-59057 *(https://www.cve.org/CVERecord?id=CVE-2025-59057)*

DESCRIPTION: React Router is a router for React. In @remix-run/react versions 1.15.0 through 2.17.0. and react-router versions 7.0.0 through 7.8.2, a XSS vulnerability exists in in React Router's meta()/Meta APIs in Framework Mode when generating script:ld+json tags which could allow arbitrary JavaScript execution during SSR if untrusted content is used to generate the tag. There is no impact if the application is being used in Declarative Mode (BrowserRouter) or Data Mode (createBrowserRouter/RouterProvider). This issue has been patched in @remix-run/react version 2.17.1 and react-router version 7.9.0.

CWE: CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(https://cwe.mitre.org/data/definitions/79.html)*

CVSS Source: security-advisories@github.com

CVSS Base score: 7.6

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

CVEID: CVE-2025-68470 *(https://www.cve.org/CVERecord?id=CVE-2025-68470)*

DESCRIPTION: React Router is a router for React. In versions 6.0.0 through 6.30.1 and 7.0.0 through 7.9.5, an attacker-supplied path can be crafted so that when a React Router application navigates to it via navigate(), Link, or redirect(), the app performs a navigation/redirect to an external URL. This is only an issue if you are passing untrusted content into navigation paths in your application code. This issue has been patched in

versions 6.30.2 and 7.9.6.

CWE: CWE-601: URL Redirection to Untrusted Site ('Open Redirect') *(https://cwe.mitre.org/data/definitions/601.html)*

CVSS Source: security-advisories@github.com

CVSS Base score: 6.5

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

CVEID: CVE-2026-21884 *(https://www.cve.org/CVERecord?id=CVE-2026-21884)*

DESCRIPTION: React Router is a router for React. In @remix-run/react version prior to 2.17.3. and react-router 7.0.0 through 7.11.0, a XSS vulnerability exists in in React Router's ScrollRestoration API in Framework Mode when using the getKey/storageKey props during Server-Side Rendering which could allow arbitrary JavaScript execution during SSR if untrusted content is used to generate the keys. There is no impact if server-side rendering in Framework Mode is disabled, or if Declarative Mode (BrowserRouter) or Data Mode (createBrowserRouter/RouterProvider) is being used. This issue has been patched in @remix-run/react version 2.17.3 and react-router version 7.12.0.

CWE: CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(https://cwe.mitre.org/data/definitions/79.html)*

CVSS Source: security-advisories@github.com

CVSS Base score: 8.2

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

CVEID: CVE-2026-22029 *(https://www.cve.org/CVERecord?id=CVE-2026-22029)*

DESCRIPTION: React Router is a router for React. In @remix-run/router version prior to 1.23.2. and react-router 7.0.0 through 7.11.0, React Router (and Remix v1/v2) SPA open navigation redirects originating from loaders or actions in Framework Mode, Data Mode, or the unstable RSC modes can result in unsafe URLs causing unintended javascript execution on the client. This is only an issue if you are creating redirect paths from untrusted content or via an open redirect. There is no impact if Declarative Mode (BrowserRouter) is being used. This issue has been patched in @remix-run/router version 1.23.2 and react-router version 7.12.0.

CWE: CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(https://cwe.mitre.org/data/definitions/79.html)*

CVSS Source: NVD

CVSS Base score: 6.1

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

CVEID: CVE-2026-22030 *(https://www.cve.org/CVERecord?id=CVE-2026-22030)*

DESCRIPTION: React Router is a router for React. In @remix-run/server-runtime version prior to 2.17.3. and react-router 7.0.0 through 7.11.0, React Router (or Remix v2) is vulnerable to CSRF attacks on document POST requests to UI routes when using server-side route action handlers in Framework Mode, or when using React Server Actions in the new unstable RSC modes. There is no impact if Declarative Mode (BrowserRouter) or Data Mode (createBrowserRouter/RouterProvider) is being used. This issue has been patched in @remix-run/server-runtime version 2.17.3 and react-router version 7.12.0.

CWE: CWE-346: Origin Validation Error *(https://cwe.mitre.org/data/definitions/346.html)*

CVSS Source: security-advisories@github.com
CVSS Base score: 6.5
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N)

CVEID: CVE-2025-47907 *(https://www.cve.org/CVERecord?id=CVE-2025-47907)*
DESCRIPTION: Cancelling a query (e.g. by cancelling the context passed to one of the query methods) during a call to the Scan method of the returned Rows can result in unexpected results if other queries are being made in parallel. This can result in a race condition that may overwrite the expected results with those of another query, causing the call to Scan to return either unexpected results from the other query or an error.
CWE: CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(https://cwe.mitre.org/data/definitions/362.html)*
CVSS Source: CISA ADP
CVSS Base score: 7
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L)

CVEID: CVE-2025-61723 *(https://www.cve.org/CVERecord?id=CVE-2025-61723)*
DESCRIPTION: The processing time for parsing some invalid inputs scales non-linearly with respect to the size of the input. This affects programs which parse untrusted PEM inputs.
CWE: CWE-770: Allocation of Resources Without Limits or Throttling *(https://cwe.mitre.org/data/definitions/770.html)*
CVSS Source: CISA ADP
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-2025-58187 *(https://www.cve.org/CVERecord?id=CVE-2025-58187)*
DESCRIPTION: Due to the design of the name constraint checking algorithm, the processing time of some inputs scale non-linearly with respect to the size of the certificate. This affects programs which validate arbitrary certificate chains.
CWE: CWE-407: Inefficient Algorithmic Complexity *(https://cwe.mitre.org/data/definitions/407.html)*
CVSS Source: CISA ADP
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-2025-69223 *(https://www.cve.org/CVERecord?id=CVE-2025-69223)*
DESCRIPTION: AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Versions 3.13.2 and below allow a zip bomb to be used to execute a DoS against the AIOHTTP server. An attacker may be able to send a compressed request that when decompressed by AIOHTTP could exhaust the host's memory. This issue is fixed in version 3.13.3.
CWE: CWE-409: Improper Handling of Highly Compressed Data (Data Amplification) *(https://cwe.mitre.org/data/definitions/409.html)*
CVSS Source: security-advisories@github.com
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-2025-69224 *(https://www.cve.org/CVERecord?id=CVE-2025-69224)*

DESCRIPTION: AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Versions 3.13.2 and below of the Python HTTP parser may allow a request smuggling attack with the presence of non-ASCII characters. If a pure Python version of AIOHTTP is installed (i.e. without the usual C extensions) or AIOHTTP_NO_EXTENSIONS is enabled, then an attacker may be able to execute a request smuggling attack to bypass certain firewalls or proxy protections. This issue is fixed in version 3.13.3.

CWE: CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') *(https://cwe.mitre.org/data/definitions/444.html)*

CVSS Source: NVD

CVSS Base score: 6.5

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

CVEID: CVE-2025-69225 *(https://www.cve.org/CVERecord?id=CVE-2025-69225)*

DESCRIPTION: AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Versions 3.13.2 and below contain parser logic which allows non-ASCII decimals to be present in the Range header. There is no known impact, but there is the possibility that there's a method to exploit a request smuggling vulnerability. This issue is fixed in version 3.13.3.

CWE: CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') *(https://cwe.mitre.org/data/definitions/444.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)

CVEID: CVE-2025-69226 *(https://www.cve.org/CVERecord?id=CVE-2025-69226)*

DESCRIPTION: AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Versions 3.13.2 and below enable an attacker to ascertain the existence of absolute path components through the path normalization logic for static files meant to prevent path traversal. If an application uses web.static() (not recommended for production deployments), it may be possible for an attacker to ascertain the existence of path components. This issue is fixed in version 3.13.3.

CWE: CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(https://cwe.mitre.org/data/definitions/22.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:L/I:N/A:N)

CVEID: CVE-2025-69227 *(https://www.cve.org/CVERecord?id=CVE-2025-69227)*

DESCRIPTION: AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Versions 3.13.2 and below allow for an infinite loop to occur when assert statements are bypassed, resulting in a DoS attack when processing a POST body. If optimizations are enabled (-O or PYTHONOPTIMIZE=1), and the

application includes a handler that uses the Request.post() method, then an attacker may be able to execute a DoS attack with a specially crafted message. This issue is fixed in version 3.13.3.

CWE: CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') *(https://cwe.mitre.org/data/definitions/835.html)*

CVSS Source: NVD

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-2025-69228 *(https://www.cve.org/CVERecord?id=CVE-2025-69228)*

DESCRIPTION: AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Versions 3.13.2 and below allow a request to be crafted in such a way that an AIOHTTP server's memory fills up uncontrollably during processing. If an application includes a handler that uses the Request.post() method, an attacker may be able to freeze the server by exhausting the memory. This issue is fixed in version 3.13.3.

CWE: CWE-770: Allocation of Resources Without Limits or Throttling *(https://cwe.mitre.org/data/definitions/770.html)*

CVSS Source: NVD

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-2025-69229 *(https://www.cve.org/CVERecord?id=CVE-2025-69229)*

DESCRIPTION: AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. In versions 3.13.2 and below, handling of chunked messages can result in excessive blocking CPU usage when receiving a large number of chunks. If an application makes use of the request.read() method in an endpoint, it may be possible for an attacker to cause the server to spend a moderate amount of blocking CPU time (e.g. 1 second) while processing the request. This could potentially lead to DoS as the server would be unable to handle other requests during that time. This issue is fixed in version 3.13.3.

CWE: CWE-770: Allocation of Resources Without Limits or Throttling *(https://cwe.mitre.org/data/definitions/770.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:N/A:L)

CVEID: CVE-2025-69230 *(https://www.cve.org/CVERecord?id=CVE-2025-69230)*

DESCRIPTION: AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. In versions 3.13.2 and below, reading multiple invalid cookies can lead to a logging storm. If the cookies attribute is accessed in an application, then an attacker may be able to trigger a storm of warning-level logs using a specially crafted Cookie header. This issue is fixed in 3.13.3.

CWE: CWE-779: Logging of Excessive Data *(https://cwe.mitre.org/data/definitions/779.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:L/I:N/A:N)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Concert Software	1.0.0-2.2.0

Remediation/Fixes

IBM strongly recommends addressing the vulnerability now by upgrading to IBM Concert Software 2.3.1

Download IBM Concert Software 2.3.1 from Container software library section of IBM Entitled Registry (ICR *(https://myibm.ibm.com/products-services/containerlibrary)*) and follow installation instructions *(https://www.ibm.com/docs/en/concert?topic=installing-preparing-run-installs-from-private-container-registry)* depending on the type of deployment.

Workarounds and Mitigations

None

Get Notified about Future Security Bulletins

Subscribe to My Notifications *(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

Related Information

IBM Secure Engineering Web Portal *(http://www.ibm.com/security/secure-engineering/bulletins.html)*
IBM Product Security Incident Response Blog *(http://www.ibm.com/blogs/psirt)*

Acknowledgement

Change History

06 Apr 2026: 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.

Document Information

More support for:
IBM Concert Software

Software version:
1.0

Operating system(s):
Linux

Document number:
7268620

Modified date:
06 April 2026

Initial Publish date:
06 April 2026