Security Bulletin: IBM MQ Operator and Queue manager container images are vulnerable to libxml2, Go JOSE and FreeType

Security Bulletin

Summary

libxml2, Go JOSE, FreeType and IBM MQ used by IBM MQ Operator and Queue Manager container images are vulnerable to memory exhaustion and a Denial of Service by sending numerous malformed tokens, and arbitrary code execution by writing up to 6 signed long integers out of bounds. This bulletin identifies the steps required to address these vulnerabilities.

Vulnerability Details

CVEID: CVE-2025-27365 *(https://www.cve.org/CVERecord?id=CVE-2025-27365)*
DESCRIPTION: An IBM WebSphere MQ Client connecting to a MQ Queue Manager can cause a SIGSEGV in the AMQRMPPA channel process terminating it.
CWE: CWE-416: Use After Free *(https://cwe.mitre.org/data/definitions/416.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-2024-56171 *(https://www.cve.org/CVERecord?id=CVE-2024-56171)*
DESCRIPTION: libxml2 before 2.12.10 and 2.13.x before 2.13.6 has a use-after-free in xmlSchemaIDCFillNodeTables and xmlSchemaBubbleIDCNodeTables in xmlschemas.c. To exploit this, a crafted XML document must be validated against an XML schema with certain identity constraints, or a crafted XML schema must be used.
CWE: CWE-416: Use After Free *(https://cwe.mitre.org/data/definitions/416.html)*
CVSS Source: cve@mitre.org
CVSS Base score: 7.8
CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N)

CVEID: CVE-2025-1333 *(https://www.cve.org/CVERecord?id=CVE-2025-1333)*
DESCRIPTION: IBM MQ Container when used with the MQ Operator and configured with Cloud Pak for Integration Keycloak could disclose sensitive information to a privileged user.
CWE: CWE-214: Invocation of Process Using Visible Sensitive Information *(https://cwe.mitre.org/data/definitions/214.html)*
CVSS Source: IBM

CVSS Base score: 6

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

CVEID: CVE-2025-27144 *(https://www.cve.org/CVERecord?id=CVE-2025-27144)*

DESCRIPTION: Go JOSE provides an implementation of the Javascript Object Signing and Encryption set of standards in Go, including support for JSON Web Encryption (JWE), JSON Web Signature (JWS), and JSON Web Token (JWT) standards. In versions on the 4.x branch prior to version 4.0.5, when parsing compact JWS or JWE input, Go JOSE could use excessive memory. The code used strings.Split(token, ".") to split JWT tokens, which is vulnerable to excessive memory consumption when processing maliciously crafted tokens with a large number of `.` characters. An attacker could exploit this by sending numerous malformed tokens, leading to memory exhaustion and a Denial of Service. Version 4.0.5 fixes this issue. As a workaround, applications could pre-validate that payloads passed to Go JOSE do not contain an excessive number of `.` characters.

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

CVSS Source: security-advisories@github.com

CVSS Base score: 6.6

CVSS Vector:
(CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X)

CVEID: CVE-2019-11777 *(https://www.cve.org/CVERecord?id=CVE-2019-11777)*

DESCRIPTION: Eclipse Paho Java client could allow a remote attacker to bypass security restrictions, caused by the failure to check the result when connecting to an MQTT server using TLS and setting a host name verifier. By sending a specially-crafted request, an attacker could exploit this vulnerability to allow one MQTT server to impersonate another and provide the client library with incorrect information.

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

CVSS Source: IBM X-Force

CVSS Base score: 7.5

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

CVEID: 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)*

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-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)*

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-2025-24928 *(https://www.cve.org/CVERecord?id=CVE-2025-24928)*

DESCRIPTION: libxml2 before 2.12.10 and 2.13.x before 2.13.6 has a stack-based buffer overflow in xmlSnprintfElements in valid.c. To exploit this, DTD validation must occur for an untrusted document or untrusted DTD. NOTE: this is similar to CVE-2017-9047.

CWE: CWE-121: Stack-based Buffer Overflow *(https://cwe.mitre.org/data/definitions/121.html)*

CVSS Source: cve@mitre.org

CVSS Base score: 7.8

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

CVEID: CVE-2025-27363 *(https://www.cve.org/CVERecord?id=CVE-2025-27363)*

DESCRIPTION: An out of bounds write exists in FreeType versions 2.13.0 and below (newer versions of FreeType are not vulnerable) when attempting to parse font subglyph structures related to TrueType GX and variable font files. The vulnerable code assigns a signed short value to an unsigned long and then adds a static value causing it to wrap around and allocate too small of a heap buffer. The code then writes up to 6 signed long integers out of bounds relative to this buffer. This may result in arbitrary code execution. This vulnerability may have been exploited in the wild.

CWE: CWE-787: Out-of-bounds Write *(https://cwe.mitre.org/data/definitions/787.html)*

CVSS Source: cve-assign@fb.com

CVSS Base score: 8.1

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

Affected Products and Versions

Affected Product(s)	Version(s)
IBM MQ Operator	SC2: v3.2.0 - v3.2.10 CD: v3.0.0, v3.0.1, v3.1.0 - 3.1.3, v3.3.0, v3.4.0, v3.4.1, v3.5.0, v3.5.1 LTS: v2.0.0 - 2.0.29 Other Release: v2.4.0 - v2.4.8, v2.3.0 - 2.3.3, v2.2.0 - v2.2.2
IBM supplied MQ Advanced container images	CD: 9.3.4.0-r1, 9.3.4.1-r1, 9.3.5.0-r1, 9.3.5.0-r2, 9.3.5.1-r1, 9.3.5.1-r2, 9.4.1.0-r1, 9.4.1.0-r2, 9.4.1.1-r1, 9.4.2.0-r1, 9.4.2.0-r2

	LTS: 9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.0.10-r2, 9.3.0.11-r1,9.3.0.11-r2, 9.3.0.15-r1, 9.3.0.16-r1, 9.3.0.16-r2, 9.3.0.17-r1, 9.3.0.17-r2, 9.3.0.17-r3, 9.3.0.20-r1, 9.3.0.20-r2, 9.3.0.21-r1, 9.3.0.21-r2, 9.3.0.21-r3, 9.3.0.25-r1, 9.4.0.0-r1, 9.4.0.0-r2, 9.4.0.0-r3, 9.4.0.5-r1, 9.4.0.5-r2, 9.4.0.6-r1, 9.4.0.6-r2, 9.4.0.7-r1, 9.4.0.10-r1, 9.4.0.10-r2 Other Release: 9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.1.0-r1, 9.3.1.0-r2, 9.3.1.0-r3, 9.3.1.1-r1, 9.3.2.0-r1, 9.3.2.0-r2, 9.3.2.1-r1, 9.3.2.1-r2, 9.3.3.0-r1, 9.3.3.0-r2, 9.3.3.1-r1, 9.3.3.1-r2, 9.3.3.2-r1, 9.3.3.2-r2, 9.3.3.2-r3, ,9.3.3.3-r1, 9.3.3.3-r2

Remediation/Fixes

Issues mentioned by this security bulletin are addressed in -

- IBM MQ Operator v3.5.2 CD release that included IBM supplied MQ Advanced 9.4.2.1-r1 container image.
- IBM MQ Operator v3.2.11 SC2 release that included IBM supplied MQ Advanced 9.4.0.11-r1 container image.
- IBM MQ Container 9.4.2.1-r1 release.

IBM strongly recommends applying the latest container images.

IBM MQ Operator v3.5.2 CD release details:

Image	Fix Version	Registry	Image Location
ibm-mq-operator	v3.5.2	icr.io	icr.io/cpopen/ibm-mq-operator@sha256:0dd8e78d3abce6120bb93bdf0b50dc4fe46c2dccfe4bed2c131d5
ibm-mqadvanced-	9.4.2.1-	cp.icr.io	cp.icr.io/cp/ibm-mqadvanced-

server	r1		server@sha256:db6edb4f68f41c97bfe08a9326c6344d19c5832907a7af45b1c641c
ibm-mqadvanced-server-integration	9.4.2.1-r1	cp.icr.io	cp.icr.io/cp/ibm-mqadvanced-server-integration@sha256:ca31e51d125558c6e6949f20adaa386307056e14bb80ef2ebd
ibm-mqadvanced-server-dev	9.4.2.1-r1	icr.io	icr.io/ibm-messaging/ibm-mqadvanced-server-dev@sha256:4a0f207897b650841a566b6acd7e5701dc8a0e11e617be1963dcc33

IBM MQ Operator v3.2.11 SC2 release details:

Image	Fix Version	Registry	Image Location
ibm-mq-operator	v3.2.11	icr.io	icr.io/cpopen/ibm-mq-operator@sha256:21c814497aee2c0eb59b090d407d52afdf94a9a80d77db609ca
ibm-mqadvanced-server	9.4.0.11-r1	cp.icr.io	cp.icr.io/cp/ibm-mqadvanced-server@sha256:d238707b997f823b661a95d00b26f84b8e20bb838066ddbc87e82
ibm-mqadvanced-server-integration	9.4.0.11-r1	cp.icr.io	cp.icr.io/cp/ibm-mqadvanced-server-integration@sha256:f69fc7dcdec9af8010a19ff14ecaab6c81c1b59f386bb6a69027
ibm-mqadvanced-server-dev	9.4.0.11-r1	icr.io	icr.io/ibm-messaging/ibm-mqadvanced-server-dev@sha256:61686e2f37f47f44c4bd1467a4d3c4bb67d197f906d6b2161acdffdffb

IBM MQ Container 9.4.2.1-r1 release details:

Image	Fix Version	Registry	Image Location
ibm-mqadvanced-server	9.4.2.1-r1	cp.icr.io	cp.icr.io/cp/ibm-mqadvanced-server@sha256:db6edb4f68f41c97bfe08a9326c6344d19c5832907a7af45b1c641c

ibm-mqadvanced-server-dev	9.4.2.1-r1	icr.io	icr.io/ibm-messaging/ibm-mqadvanced-server-dev@sha256:4a0f207897b650841a566b6acd7e5701dc8a0e11e617be1963dcc33

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

https://access.redhat.com/errata/RHSA-2025:3407 *(https://access.redhat.com/errata/RHSA-2025:3407)*
https://access.redhat.com/errata/RHSA-2025:2679 *(https://access.redhat.com/errata/RHSA-2025:2679)*
https://access.redhat.com/errata/RHSA-2025:2679 *(https://access.redhat.com/errata/RHSA-2025:2679)*
https://access.redhat.com/errata/RHSA-2025:3335 *(https://access.redhat.com/errata/RHSA-2025:3335)*

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

01 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.

Document Information

More support for:

IBM MQ container software *(https://www.ibm.com/mysupport/s/topic/0TO5000000024cJGAQ)*

Software version:

IBM MQ Operator v3.5.2, IBM MQ Operator v3.2.11, IBM MQ Container 9.4.2.1-r1

Operating system(s):

RedHat OpenShift

Document number:

7232272

Modified date:

01 May 2025