RABBITMQ SECURITY INTELLIGENCE SERIES

RabbitMQ CVE Register and Risk Report

Every published RabbitMQ security advisory, mapped to version and severity.

ABOUT THIS REPORT

Source **rabbitmq.com/security (GitHub Security Advisories)**
Coverage **2021-06-27 through 2026-06-24**
Advisories tracked **21 published CVEs**
Prepared by **AceMQ Engineering**
Edition **July 2026**

INTRODUCTION

Twenty-one advisories, one clear pattern

This report consolidates every publicly disclosed RabbitMQ security advisory listed on Broadcom's official RabbitMQ security page into a single register, cross-referenced against the version series it affects. It is built for the same audience that reads a patch note before a maintenance window: precise, sourced, and free of marketing language.

As of this edition there are 21 published open-source advisories spanning 2021 through 2026, covering the core broker (rabbitmq-server) and the Java client library. No Critical-severity advisory has been published to date; the highest published severity is High.

SCOPE AND A NOTE ON DOUBLE-COUNTING

Commercial VMware Tanzu RabbitMQ customers should treat the Broadcom Support Portal as authoritative, since it includes CVEs in dependencies and the underlying Erlang runtime not listed on the public page this report is built from.

Most advisories were backported across several release series at once. In the per-version chart and table later in this report, a single CVE is counted once for every series it was patched in, because each series needed its own independent fix and upgrade. That is why the sum across all version rows (49) is larger than the count of unique advisories (21).

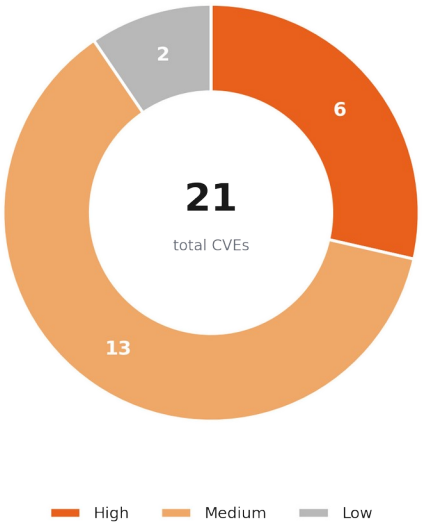
What is inside

Section One Severity and timeline overview, with the full distribution chart
Section Two CVEs per version series, with the stacked severity chart and summary table
Section Three The complete CVE register: every advisory, clickable, with affected and patched versions
Section Four How to read this for a patching decision, and where AceMQ fits

SECTION ONE

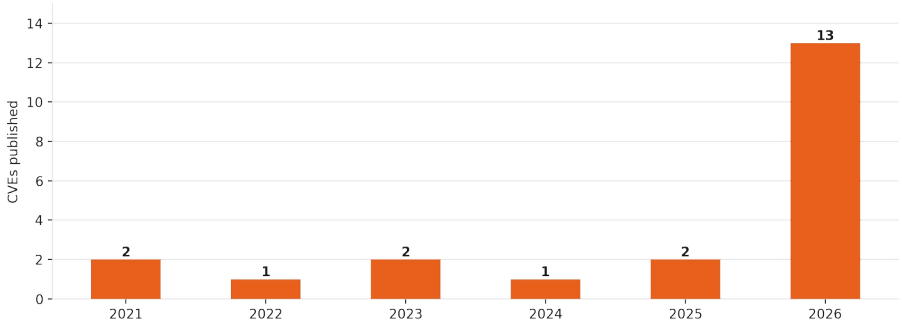
Severity distribution and publication timeline

Twenty-one advisories break down as follows. Medium severity dominates, largely driven by management-UI XSS findings and authorization edge cases. Six advisories are rated High, generally involving authentication bypass, cross-tenant data exposure, or denial of service. No Critical-severity advisory has been published against RabbitMQ to date.



Advisories by year

Publication volume rose sharply in 2026: eleven of the twenty-one advisories in this register, more than half, were published between May and June of 2026 alone, largely as a coordinated disclosure batch affecting the 3.13, 4.0, 4.1, and 4.2 series together.



SECTION TWO

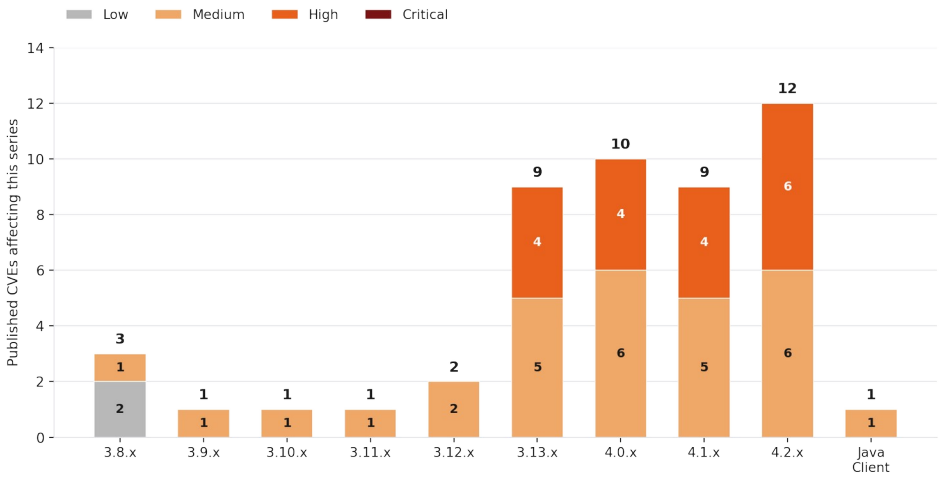
CVEs per Version and Severity

Every release series, broken down by Critical, High, Medium, and Low

SECTION TWO

Where the exposure concentrates

The chart below plots every published CVE against the version series it affects. Because most 2026 advisories were backported across four release lines at once, the actively maintained series (3.13, 4.0, 4.1, 4.2) carry the highest counts, not because they are less secure, but because they are the versions still receiving patches. Retired series (3.8 through 3.12) stopped accumulating new advisories once they passed end of community support.



Summary table

Each row counts unique CVEs that required a patch release on that series. A CVE affecting four series appears once in each of the four rows below, consistent with the chart above.

VERSION SERIES	CRITICAL	HIGH	MEDIUM	LOW	TOTAL CVES
3.8.x	0	0	1	2	**3**
3.9.x	0	0	1	0	**1**
3.10.x	0	0	1	0	**1**
3.11.x	0	0	1	0	**1**
3.12.x	0	0	2	0	**2**
3.13.x	0	4	5	0	**9**
4.0.x	0	4	6	0	**10**
4.1.x	0	4	5	0	**9**
4.2.x	0	6	6	0	**12**
Java Client (rabbitmq-java-client)	0	0	1	0	**1**

READING THIS TABLE

4.2.x carries the highest total (12) because it is the current release series and therefore the target of every 2026 backport. 3.13.x, 4.0.x, and 4.1.x each carry 9 to 10, reflecting the same batch of advisories patched across all supported branches.

3.8.x through 3.12.x are retired series. Their low counts reflect a shorter window of active disclosure, not stronger security, since Broadcom stopped backporting new fixes to them once each series reached end of life.

SECTION THREE

The Complete CVE Register

All 21 published advisories, most recent first

SECTION THREE

Full register, sourced from rabbitmq.com/security

Every CVE ID below links directly to its GitHub Security Advisory. Repository names link to the source repository. Affected and patched versions are quoted as published; where Broadcom lists an enterprise-only patched build, that is noted in the source page linked from each advisory.

CVE ID	PUBLISHED	SEVERITY	REPOSITORY	SUMMARY	AFFECTED VERSIONS	PATCHED VERSIONS
CVE-2026-57215	2026-06-24	HIGH	rabbitmq-server	Direct-reply-to binding persistence can lead to unauthorized reply-channel injection and persistent phantom binding.	4.2.0 - 4.2.5, 4.1.0 - 4.1.10, 4.0.0 - 4.0.19, 3.13.0 - 3.13.14	**4.2.6, 4.1.11, 4.0.20, 3.13.15**
CVE-2026-57216	2026-06-24	MEDIUM	rabbitmq-server	AMQP 1.0, AMQP 0-9-1, and Stream protocol loopback enforcement can lead to remote guest sessions due to listener-address loopback checks.	4.2.0 - 4.2.5, 4.1.0 - 4.1.10, 4.0.0 - 4.0.19, 3.13.0 - 3.13.14	**4.2.6, 4.1.11, 4.0.20, 3.13.15**
CVE-2026-57217	2026-06-24	HIGH	rabbitmq-server	Topic authorization can lead to cross-tenant routing-key bypass.	4.2.0 - 4.2.5, 4.1.0 - 4.1.10, 4.0.0 - 4.0.20, 3.13.0 - 3.13.14	**4.2.6, 4.1.11, 4.0.21, 3.13.15**
CVE-2026-57218	2026-06-24	MEDIUM	rabbitmq-server	AMQP 0-9-1 in combination with OAuth 2: consumer persistence can lead to post-revocation message disclosure.	4.2.0 - 4.2.5	**4.2.6**
CVE-2026-57220	2026-06-24	HIGH	rabbitmq-server	Stream listener does not enforce the configured frame-size limit during authentication, permitting an unauthenticated memory-exhaustion DoS.	4.2.0 - 4.2.5	**4.2.6**
CVE-2026-57221	2026-06-24	MEDIUM	rabbitmq-server	Passive queue/exchange declaration bypasses authorization checks, leaking queue metadata to unprivileged users.	4.2.0 - 4.2.5, 4.1.0 - 4.1.10, 4.0.0 - 4.0.19, 3.13.0 - 3.13.14	**4.2.6, 4.1.11, 4.0.20, 3.13.15**
CVE-2026-57219	2026-06-24	HIGH	rabbitmq-server	Unauthenticated disclosure of OAuth client credentials via an HTTP API endpoint under certain less common OAuth 2 configurations.	4.2.0 - 4.2.5, 4.1.0 - 4.1.10, 4.0.0 - 4.0.19, 3.13.0 - 3.13.14	**4.2.6, 4.1.11, 4.0.20, 3.13.15**
CVE-2026-57214	2026-06-18	HIGH	rabbitmq-server	Stored XSS in the RabbitMQ management UI.	4.2.0 - 4.2.4	**4.2.5**
CVE-2026-57213	2026-06-18	MEDIUM	rabbitmq-server	Stored XSS in the RabbitMQ federation management plugin via unsanitized consumer_tag rendering.	4.2.0 - 4.2.4, 4.1.0 - 4.1.9, 4.0.0 - 4.0.18, 3.13.0 - 3.13.13	**4.2.5, 4.1.10, 4.0.19, 3.13.14**
CVE-2026-	2026-06-	HIGH	rabbitmq-server	RabbitMQ management HTTP API accepts request bodies	4.2.0 - 4.2.4, 4.1.0 -	**4.2.5, 4.1.10, 4.0.19,**

CVE ID	PUBLISHED	SEVERITY	REPOSITORY	SUMMARY	AFFECTED VERSIONS	PATCHED VERSIONS
57212	18			larger than the configured max_http_body_size.	4.1.9, 4.0.0 - 4.0.18, 3.13.0 - 3.13.13	**3.13.14**
CVE-2026-57211	2026-06-18	MEDIUM	rabbitmq-server	UNC SSRF affecting the RabbitMQ management UI on Windows.	4.2.0 - 4.2.5, 4.1.0 - 4.1.10	**4.2.6, 4.1.11**
CVE-2026-44839	2026-05-06	MEDIUM	rabbitmq-server	Unsanitized vhost names allow for XSS in the management UI.	4.1.0 - 4.1.1, 4.0.0 - 4.0.12	**4.1.2, 4.0.13**
CVE-2026-44838	2026-05-06	MEDIUM	rabbitmq-server	RabbitMQ MQTT topic permission authorization bypass.	4.2.0 - 4.2.3	**4.2.4**
CVE-2025-50200	2025-06-18	MEDIUM	rabbitmq-server	Node can log the Basic Auth header from an HTTP request.	4.0.0 - 4.0.7, 3.13.0 - 3.13.7	**4.0.8, 3.13.8**
CVE-2025-30219	2025-03-25	MEDIUM	rabbitmq-server	XSS vulnerability in an error message in the management UI.	4.0.0 - 4.0.2, 3.13.0 - 3.13.7	**4.0.3, 3.13.8**
CVE-2024-51988	2024-11-06	MEDIUM	rabbitmq-server	HTTP API's queue deletion endpoint does not verify that the user has the required permission.	> 3.12.7, < 3.12.11	**3.12.11**
CVE-2023-46118	2023-10-23	MEDIUM	rabbitmq-server	Denial of service by publishing large messages over the HTTP API.	3.12.0 - 3.12.6, 3.11.0 - 3.11.23	**3.12.7, 3.11.24**
CVE-2023-46120	2023-10-23	MEDIUM	rabbitmq-java-client	No message size limit in the RabbitMQ Java client can lead to a remote DoS attack on consumer applications.	< 5.18.0	**5.18.0**
CVE-2022-31008	2022-10-05	MEDIUM	rabbitmq-server	Predictable credential obfuscation seed value used in the Shovel and Federation plugins.	3.10.0 - 3.10.1, 3.9.0 - 3.9.17, 3.8.0 - 3.8.31	**3.10.2, 3.9.18, 3.8.32**
CVE-2021-32718	2021-06-27	LOW	rabbitmq-server	Improper neutralization of script-related HTML tags in a web page (basic XSS) in the RabbitMQ management UI.	< 3.8.17	**3.8.17**
CVE-2021-32719	2021-06-27	LOW	rabbitmq-server	Improper neutralization of script-related HTML tags in a web page (basic XSS) in the RabbitMQ federation management plugin.	< 3.8.18	**3.8.18**

SECTION FOUR

Turning this register into a patch decision

A CVE list is only useful if it changes what you do next. Three questions determine priority for any RabbitMQ estate:

Is the affected series still in my environment? Cross-reference the version series table in Section Two against your fleet inventory. Anything on 3.8 through 3.12 is on a retired series; those advisories are historical exposure only if you have already upgraded.

Is the vulnerable surface actually exposed? Several 2026 advisories require management UI access, a specific OAuth 2 configuration, or Windows-specific UNC handling. Confirm the precondition applies before treating every row as equally urgent.

Is my patched version current? The Patched Versions column in Section Three is the floor, not a target. Always apply the latest release in your series rather than the minimum patched version, since later releases fold in every prior fix.

Extended support changes this calculus

Teams on a retired series (3.8 through 3.12, or an end-of-support 3.13/4.x build) face a choice between an urgent version upgrade or a CVE-patched Extended Long-Term Support build that backports exactly these fixes without a full version migration. This is frequently the faster and lower-risk path when an upgrade window is not immediately available.

> **WHERE ACEMQ FITS**
>
> AceMQ is the world's only Broadcom-authorized Tanzu RabbitMQ Managed Services Provider. We track every advisory in this register against our managed clusters the day it publishes, and back-check affected version ranges against actual client fleets rather than assuming exposure.
>
> For teams on a retired series, our Extended LTS offering delivers CVE-patched builds without forcing an immediate major-version migration. For teams on a current series, we validate patch levels during every engagement and flag drift before it becomes exposure.
>
> Need a fleet-wide exposure check against this register, or a migration plan off a retired series? That is exactly the work we do every day.

Talk to AceMQ

AceMQ, an ace8 company

66 W. Flagler St., 9th Floor, Miami, FL 33130

305-204-2607 · info@acemq.com · acemq.com

Source: rabbitmq.com/security

Data current as of the publication date on the source page. Verify against the live page before a compliance submission, as new advisories publish on an ongoing basis.