Distributed Message Service for RabbitMQ

Bulletin

Issue 01

Date 2025-12-22

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Vulnerability Notice....1
1.1 Vulnerability Fixing Policies....1
2 Version Notes....2
2.1 Version Support Notes....2
2.2 Release Notes....3

1 Vulnerability Notice

1.1 Vulnerability Fixing Policies

Vulnerability Fixing SLA

- High-risk vulnerabilities

  Distributed Message Service (DMS) for RabbitMQ fixes vulnerabilities within one month after the RabbitMQ community detects them and releases fixing solutions. The fixing policies are the same as those of the community.

  An emergent OS vulnerability will be released in line with the related policies and process. A fix will be provided in about one month. You can fix the vulnerability on your own.

- Other vulnerabilities

  Upgrade versions to fix other vulnerabilities.

Fixing Statement

To prevent customers from being exposed to unexpected risks, DMS for RabbitMQ does not provide other information about vulnerabilities except the vulnerability background, details, technical analysis, affected functions/versions/scenarios, solutions, and reference information.

In addition, DMS for RabbitMQ provides the same information for all customers to protect all customers equally. DMS for RabbitMQ will not notify individual customers in advance.

DMS for RabbitMQ does not develop or release intrusive code (or code for verification) to exploit vulnerabilities.

2 Version Notes

2.1 Version Support Notes

Description

The version number of DMS for RabbitMQ is in format **message engine x.y.z**. The message engine is RabbitMQ. **Figure 2-1** describes a RabbitMQ version.

Figure 2-1 Version number sample

Supported Versions

3.8.35 and AMQP-0-9-1

Version Lifecycle

Table 2-1 lists the lifecycle of DMS for RabbitMQ versions.

Table 2-1 Version lifecycle

Message Engine	Version	Status	Commercial Release	EOM	EOS
RabbitMQ	3.7.17	EOM	October 2019	October 2022	September 2025
	3.8.35	On sale	September 2022	N/A	N/A
	AMQP-0-9-1	On sale	October 2024	N/A	N/A

NOTE

- EOM: End of marketing.
- EOS: End of service & support. It is recommended that you use the latest message engine. No technical support services will be provided for this version after this date.

2.2 Release Notes

Table 2-2 lists the new and optimized features of DMS for RabbitMQ compared with open-source RabbitMQ.

Table 2-2 Release notes

Version	Release Date	New/Optimized Feature
3.8.35	February 2023	Broker flavor increase/decrease
3.8.35	December 2022	Virtual host management on the console
3.8.35	September 2022	Single active consumer and quorum queue

