Distributed Cache Service

Product Bulletin

Issue 01

Date 2023-07-25

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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 Notices

1.1 Vulnerability Fixing Policies

Vulnerability Fixing Time

- High-risk vulnerabilities

  After the Redis community detects vulnerabilities and releases fixing solutions, Distributed Cache Service (DCS) fixes the vulnerabilities according the community's policies and fully verifies the Redis kernel changes within one to three months.

- Other vulnerabilities

  Upgrade versions to fix other vulnerabilities.

Fixing Statement

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

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

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