



CVE-2021-31294

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-31294
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-15 23:15:00 UTC
Updated	2023-08-14 19:15:00 UTC
Description	Redis before 6cbea7d allows a replica to cause an assertion failure in a primary server by sending a non-administrative com

Risk And Classification

Problem Types: CWE-617

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redis	Redis	All	All	All	All

References

Reference	Source	Link
CVE-2021-31294 Redis Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
Prevent replicas from sending commands that interact with keyspace (#... · redis/redis@46f4ebb · GitHub	MISC	github.com
Prevent replicas from sending commands that interact with keyspace (#... · redis/redis@6cbea7d · GitHub	MISC	github.com
[CRASH]The psync command will crash redis · Issue #8712 · redis/redis · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report