



# CVE-2023-28856

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2023-28856
<b>State</b>	PUBLIC
<b>Assigner</b>	security-advisories@github.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-04-18 21:15:00 UTC
<b>Updated</b>	2023-06-01 14:15:00 UTC
<b>Description</b>	Redis is an open source, in-memory database that persists on disk. Authenticated users can use the `HINCRBYFLOAT` co

## Risk And Classification

### Problem Types: CWE-617

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	38	All	All	All
Application	<a href="#">Redis</a>	<a href="#">Redis</a>	All	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 37 Update: redis-7.0.11-1.fc37 - package-announce - Fedora Mailing-Lists	MISC	<a href="#">lists.fedor</a>
[SECURITY] Fedora 38 Update: redis-7.0.11-1.fc38 - package-announce - Fedora Mailing-Lists	MISC	<a href="#">lists.fedor</a>
HINCRBYFLOAT can be used to crash a redis-server process · Advisory · redis/redis · GitHub	MISC	<a href="#">github.co</a>
[SECURITY] [DLA 3396-1] redis security update	MISC	<a href="#">lists.debia</a>
[SECURITY] Fedora 36 Update: redis-6.2.12-1.fc36 - package-announce - Fedora Mailing-Lists	MISC	<a href="#">lists.fedor</a>
fix hincrbyfloat not to create a key if the new value is invalid (#11... · redis/redis@bc7fe41 · GitHub	MISC	<a href="#">github.co</a>
CVE-2023-28856 Redis Vulnerability in NetApp Products   NetApp Product Security	MISC	<a href="#">security.n</a>
fix hincrbyfloat not to create a key if the new value is invalid by chendq8 · Pull Request #11149 · redis/redis · GitHub	MISC	<a href="#">github.co</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[181746](#) Debian Security Update for redis (DLA 3396-1)

[184239](#) Debian Security Update for redis (CVE-2023-28856)

[199978](#) Ubuntu Security Notification for Redis Vulnerabilities (USN-6531-1)

[283943](#) Fedora Security Update for redis (FEDORA-2023-5b6510a584)

[283944](#) Fedora Security Update for redis (FEDORA-2023-04239b5758)

[284169](#) Fedora Security Update for redis (FEDORA-2023-e4e3393396)

[355163](#) Amazon Linux Security Advisory for redis6 : ALAS2023-2023-164

[691163](#) Free Berkeley Software Distribution (FreeBSD) Security Update for redis (96b2d4db-ddd2-11ed-b6ea-080027f5fec9)

[906881](#) Common Base Linux Mariner (CBL-Mariner) Security Update for redis (26267-1)

[906904](#) Common Base Linux Mariner (CBL-Mariner) Security Update for redis (26290-1)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)**