



# CVE-2021-21309

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

## Summary

<b>CVE</b>	CVE-2021-21309
<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>	2021-02-26 22:15:00 UTC
<b>Updated</b>	2022-10-19 13:21:00 UTC
<b>Description</b>	Redis is an open-source, in-memory database that persists on disk. In affected versions of Redis an integer overflow bug in

## Risk And Classification

**Problem Types:** CWE-190

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Redislabs</a>	<a href="#">Redis</a>	All	All	All	All
Application	<a href="#">Redislabs</a>	<a href="#">Redis</a>	All	All	All	All

## References

Reference	Source	Link	Tags
Redis: Remote code execution (GLSA 202103-02) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>	
Integer overflow on 32-bit systems · Advisory · redis/redis · GitHub	CONFIRM	<a href="#">github.com</a>	Third Party Advisory
Fix integer overflow. by yossigo · Pull Request #8522 · redis/redis · GitHub	MISC	<a href="#">github.com</a>	Patch, Third Party Advisory
Fix integer overflow (CVE-2021-21309). (#8522) · redis/redis@c992857 · GitHub	MISC	<a href="#">github.com</a>	Patch, Third Party Advisory
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[180059](#) Debian Security Update for redis (CVE-2021-21309)

[500599](#) Alpine Linux Security Update for redis

501481 Alpine Linux Security Update for redis
501774 Alpine Linux Security Update for redis
504353 Alpine Linux Security Update for redis
690241 Free Berkeley Software Distribution (FreeBSD) Security Update for redis (0e38b8f8-75dd-11eb-83f2-8c164567ca3c)
710008 Gentoo Linux Redis Remote Code Execution Vulnerability (GLSA 202103-02)
750019 SUSE Enterprise Linux Security Update for redis (SUSE-SU-2021:1652-1)
750226 OpenSUSE Security Update for redis (openSUSE-SU-2021:0682-1)
900042 CBL-Mariner Linux Security Update for redis 5.0.5
901260 Common Base Linux Mariner (CBL-Mariner) Security Update for redis (6843-1)
902996 Common Base Linux Mariner (CBL-Mariner) Security Update for redis (3923)

© [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](#)