



CVE-2023-45145

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

Summary

CVE	CVE-2023-45145
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-18 21:15:00 UTC
Updated	2023-11-16 15:15:00 UTC
Description	Redis is an in-memory database that persists on disk. On startup, Redis begins listening on a Unix socket before adjusting

Risk And Classification

Problem Types: CWE-668

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Operating System	Fedoraproject	Fedora	38	All	All	All
Application	Redis	Redis	All	All	All	All
Application	Redis	Redis	2.6.0	rc1	All	All

References

Reference	Source
Redis Unix-domain socket may be exposed with the wrong permissions for a short time window. · Advisory · redis/redis · GitHub	MISC
[SECURITY] [DLA 3627-1] redis security update	MISC
[SECURITY] Fedora 39 Update: redis-7.2.2-1.fc39 - package-announcement - Fedora Mailing-Lists	MISC
[SECURITY] Fedora 38 Update: redis-7.0.14-1.fc38 - package-announcement - Fedora Mailing-Lists	MISC
[SECURITY] Fedora 37 Update: redis-7.0.14-1.fc37 - package-announcement - Fedora Mailing-Lists	MISC
security.netapp.com/advisory/ntap-20231116-0014	
Fix issue of listen before chmod on Unix sockets (CVE-2023-45145) (#1... · redis/redis@03345dd · GitHub	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

199978 Ubuntu Security Notification for Redis Vulnerabilities (USN-6531-1)
284679 Fedora Security Update for redis (FEDORA-2023-77ed1e26a4)
284680 Fedora Security Update for redis (FEDORA-2023-8a9087f089)
285186 Fedora Security Update for redis (FEDORA-2023-fd75e4f307)
357096 Amazon Linux Security Advisory for redis : ALAS2REDIS6-2024-009
357116 Amazon Linux Security Advisory for redis6 : ALAS2023-2024-516
357126 Amazon Linux Security Advisory for redis6 : ALAS2023-2024-513
503397 Alpine Linux Security Update for redis
503398 Alpine Linux Security Update for redis
505930 Alpine Linux Security Update for redis
6000276 Debian Security Update for redis (DLA 3627-1)
6000455 Debian Security Update for redis (DSA 5610-1)
691329 Free Berkeley Software Distribution (FreeBSD) Security Update for redis (8706e097-6db7-11ee-8744-080027f5fec9)
755206 SUSE Enterprise Linux Security Update for redis (SUSE-SU-2023:4290-1)
755239 SUSE Enterprise Linux Security Update for redis (SUSE-SU-2023:4376-1)
755640 SUSE Enterprise Linux Security Update for redis7 (SUSE-SU-2024:0200-1)
907584 Common Base Linux Mariner (CBL-Mariner) Security Update for redis (31653-1)

© [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](#)