



CVE-2023-4322

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-4322
State	PUBLIC
Assigner	security@huntr.dev
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-14 16:15:00 UTC
Updated	2023-11-14 03:15:00 UTC
Description	Heap-based Buffer Overflow in GitHub repository radareorg/radare2 prior to 5.9.0.

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Radare	Radare2	All	All	All	All

References

Reference	Source	Link	Tags
huntr – Security Bounties for any GitHub repository	MISC	huntr.dev	
[SECURITY] Fedora 37 Update: radare2-5.8.8-2.fc37 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
Fix 1byte heap oobread in the brainfuck disassembler · radareorg/radare2@ba919ad · GitHub	MISC	github.com	
[SECURITY] Fedora 38 Update: radare2-5.8.8-2.fc38 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
CVE Program record	CVE.ORG	www.cve.org	cancel
NVD vulnerability detail	NVD	nvd.nist.gov	cancel

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[284733](#) Fedora Security Update for radare2 (FEDORA-2023-ffaebb1e10)

[284734](#) Fedora Security Update for radare2 (FEDORA-2023-f2a6d27239)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)