



CVE-2022-1714

Published on: Not Yet Published

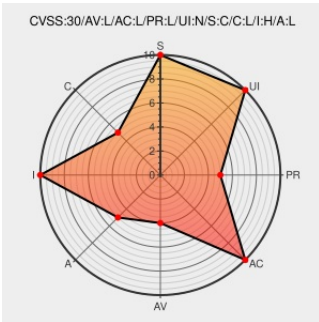
Last Modified on: 05/23/2022 06:35:00 PM UTC

CVE-2022-1714 - advisory for 1c22055b-b015-47a8-a57b-4982978751d0

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)



Certain versions of [Radare2](#) from [Radare](#) contain the following vulnerability:

Heap-based Buffer Overflow in GitHub repository radareorg/radare2 prior to 5.7.0. The bug causes the program reads data past the end of the intended buffer. Typically, this can allow attackers to read sensitive information from other memory locations or cause a crash.

CVE-2022-1714 has been assigned by security@huntr.dev to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: radareorg - radareorg/radare2 version < 5.7.0

CVSS3 Score: **7.1 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	HIGH

CVSS2 Score: **3.6 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	PARTIAL

CVE References

Description	Tags	Link
huntr – Security Bounties for any GitHub repository	huntr.dev text/html Inactive Link Not Archived	<input type="checkbox"/> CONFIRM huntr.dev/bounties/1c22055b-b015-47a8-a57b-4982978751d0

Fix 4 byte oobread in
msp430 disassembler
##crash ·
radareorg/radare2@3ecdbf8
· GitHub

[github.com](#)
[text/html](#)

MISC
github.com/radareorg/radare2/commit/3ecdbf8e21186a9c5a4d3cfa3b1e9fd270459

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:radare:radare2:*****:*.*.:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
<input type="checkbox"/> @huntrHacktivity	Heap-based Buffer Overflow in github.com/radareorg/rada... (CVE-2022-1714) reported by cnilrt - Patch:... twitter.com/i/web/status/1...	2022-05-13 14:13:16
<input type="checkbox"/> @CVEreport	CVE-2022-1714 : Heap-based Buffer Overflow in GitHub repository radareorg/radare2 prior to 5.7.0. The bug causes th... twitter.com/i/web/status/1...	2022-05-13 14:17:49
<input type="checkbox"/> /r/netcve	CVE-2022-1714	2022-05-13 15:38:18

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2022 |

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](#)