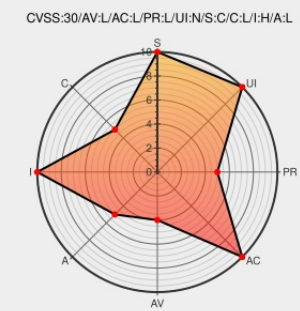
CVE-2022-1714

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 intented 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	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/3ecdbf8e21186a9c5a4d3cfa3b1e9fd270453

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)
@huntrHacktivity	Heap-based Buffer Overflow in github.com/radareorg/rada… (CVE-2022-1714) reported by cnitlrt - Patch:… twitter.com/i/web/status/1…	2022-05-13 14:13:16
@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
/r/netcve	CVE-2022-1714	2022-05-13 15:38:18

← Previous ID

Next ID→