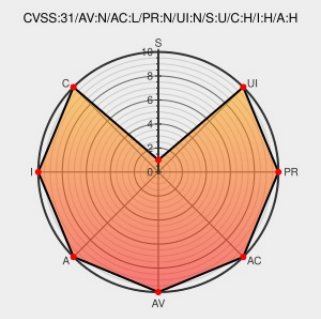
CVE-2020-24133

Published on: 07/14/2021 12:00:00 AM UTC

Last Modified on: 10/26/2022 01:48:00 PM UTC

CVE-2020-24133

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Radare2-extras from Radare contain the following vulnerability:

A heap buffer overflow vulnerability in the r_asm_swf_disass function of Radare2-extras before commit e74a93c allows attackers to execute arbitrary code or carry out denial of service (DOS) attacks.

CVE-2020-24133 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
patch Heap overflow by JJY-sec · Pull Request #255 · radareorg/radare2-extras · GitHub	github.com text/html	MISC github.com/radareorg/radare2-extras/pull/255/commits/4a8b24475549ff10bdf6d07fd4b5f6c1cc6246ea
patch Heap overflow by JJY-sec · Pull Request #255 · radareorg/radare2-extras · GitHub	github.com text/html	MISC github.com/radareorg/radare2-extras/pull/255

patch Heap overflow by JJY-sec · Pull Request #255 · radareorg/radare2-extras · GitHub	github.com text/html	MISC github.com/radareorg/radare2-extras/pull/255/commits/9f6a221433964d9b14f3ed78bc9fb059395b893b
CWE - CWE-122: Heap-based Buffer Overflow (4.3)	cwe.mitre.org text/html	MISC cwe.mitre.org/data/definitions/122.html

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-extras	All	All	All	All

cpe:2.3:a:radare:radare2-extras:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2020-24133 : A heap buffer overflow vulnerability in the r_asm_swf_disass function of Radare2-extras before com… twitter.com/i/web/status/1…	2021-07-14 22:08:33
/r/netcve	CVE-2020-24133	2021-07-14 22:41:28

← Previous ID

Next ID→