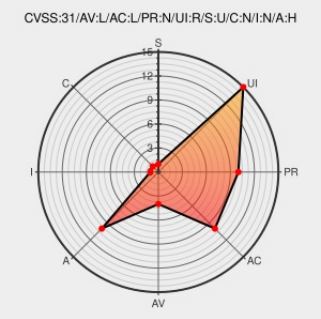
CVE-2018-20457

Published on: 12/25/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:37 PM UTC

CVE-2018-20457

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



Certain versions of Radare2 from Radare contain the following vulnerability:

In radare2 through 3.1.3, the assemble function inside libr/asm/p/asm_arm_cs.c allows attackers to cause a denial-of-service (application crash via an r_num_calc out-of-bounds read) by crafting an arm assembly input because a loop uses an incorrect index in armass.c and certain length validation is missing in armass64.c, a related issue to CVE-2018-20459.

CVE-2018-20457 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Fix #12417/#12418 (arm assembler heap overflows) ·	Patch Vendor Advisory	MISC github.com/radareorg/radare2/commit/e5c14c167b0dcf0a53d76bd50bacbbcc0dfc1ae7

radareorg/radare2@e5c14c1 · GitHub	github.com text/html	
AddressSanitizer: heap-buffer-overflow (OOB read) at libr/util/calc.c:384 · Issue #12417 · radareorg/radare2 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/radare/radare2/issues/12417

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

← Previous ID

Next ID→