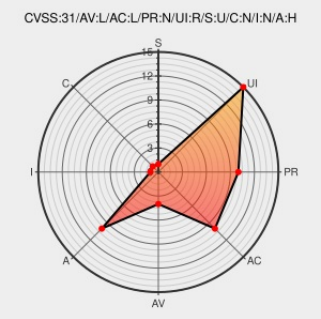
CVE-2018-20459

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

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

CVE-2018-20459

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 armass_assemble function in libr/asm/arch/arm/armass.c allows attackers to cause a denial-of-service (application crash by 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-2018-20457.

CVE-2018-20459 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
AddressSanitizer: heap-buffer-overflow (OOB read) at	Exploit Patch	MISC github.com/radare/radare2/issues/12418

libr/asm/arch/arm/armass.c:6549 · Issue #12418 · radareorg/radare2 · GitHub	Third Party Advisory github.com text/html	
Fix #12417/#12418 (arm assembler heap overflows) · radareorg/radare2@e5c14c1 · GitHub	Patch Vendor Advisory github.com text/html	MISC github.com/radareorg/radare2/commit/e5c14c167b0dcf0a53d76bd50bacbbcc0dfc1a

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→