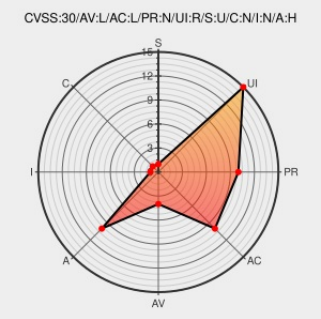
CVE-2018-11377

Published on: 05/22/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:17 PM UTC

CVE-2018-11377

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



Certain versions of Radare2 from Radare contain the following vulnerability:

The avr_op_analyze() function in radare2 2.5.0 allows remote attackers to cause a denial of service (heap-based out-of-bounds read and application crash) via a crafted binary file.

CVE-2018-11377 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 oobread in avr · radareorg/radare2@b35530f · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/radare/radare2/commit/b35530fa0681b27eba084de5527037ebfb397422

Heap out of bounds read in avr_op_analyze() · Issue #9901 · radareorg/radare2 · GitHub	Third Party Advisory github.com text/html	MISC github.com/radare/radare2/issues/9901
Fix invalid free in RAnal.avr · radareorg/radare2@25a3703 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/radare/radare2/commit/25a3703ef2e015bbe1d1f16f6b2f63bb10dd34f4

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	2.5.0	All	All	All
Application	Radare	Radare2	2.5.0	All	All	All

cpe:2.3:a:radare:radare2:2.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:radare:radare2:2.5.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→