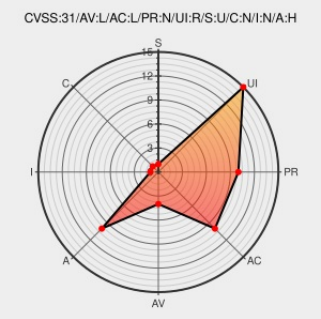
CVE-2018-14015

Published on: 07/12/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:43 PM UTC

CVE-2018-14015

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



Certain versions of Radare2 from Radare contain the following vulnerability:

The sdb_set_internal function in sdb.c in radare2 2.7.0 allows remote attackers to cause a denial of service (invalid read and application crash) via a crafted ELF file because of missing input validation in r_bin_dwarf_parse_comp_unit in libr/bin/dwarf.c.

CVE-2018-14015 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 #10465 - Avoid string on low addresses (workaround) for corrupted… · radareorg/radare2@d37d2b8 · GitHub	Patch Vendor Advisory github.com text/html	MISC github.com/radareorg/radare2/commit/d37d2b858ac47f2f108034be0bcecadaddfbc8b3

invalid read error at sdb.c:562 · Issue #10465 · radareorg/radare2 · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/radare/radare2/issues/10465

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	2.7.0	All	All	All
Application	Radare	Radare2	2.7.0	All	All	All

cpe:2.3:a:radare:radare2:2.7.0:*:*:*:*:*:*:*:

cpe:2.3:a:radare:radare2:2.7.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→