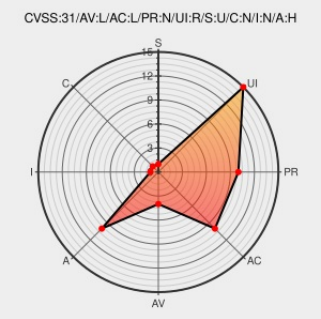
CVE-2018-14016

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

Last Modified on: 03/23/2021 11:24:42 PM UTC

CVE-2018-14016

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



Certain versions of Radare2 from Radare contain the following vulnerability:

The r_bin_mdmp_init_directory_entry function in mdmp.c in radare2 2.7.0 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted Mini Crash Dump file.

CVE-2018-14016 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
invalid read error/heap buffer overflow at mdmp.c:364 · Issue #10464 · radareorg/radare2 · GitHub	Exploit, Third Party Advisory, github.com, text/html	MISC github.com/radare/radare2/issues/10464

Fix #10464 - oobread crash in mdmp (#10683) · radareorg/radare2@eb7deb2 · GitHub	Patch Vendor Advisory github.com text/html	MISC github.com/radareorg/radare2/commit/eb7deb281df54771fb8ecf5890dc325a7d22d3e2

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→