



CVE-2017-16359

Published on: 11/01/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:38 PM UTC

CVE-2017-16359

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Radare2](#) from [Radare](#) contain the following vulnerability:

In radare 2.0.1, a pointer wraparound vulnerability exists in `store_versioninfo_gnu_verdef()` in `libr/bin/format/elf/elf.c`.

CVE-2017-16359 has been assigned by [M](#) 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 #8764 a 3rd time since 2nd time is UB and can be optimized away · radareorg/radare2@fbaf24b · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	CONFIRM github.com/radare/radare2/commit/fbaf24bce7ea4211e4608b3ab6c1b45702cb243d

Fix #8764 - huge vd_aux caused pointer wraparound · radareorg/radare2@62e39f3 · GitHub

Issue Tracking

Patch

Third Party Advisory

github.com

text/html

CONFIRM

github.com/radare/radare2/commit/62e39f34b2705131a2d08aff0c2e542c6a52cf0e

Fix #8764 differently since ptr diff might not fit in ptrdiff_t · radareorg/radare2@d21e91f · GitHub

Issue Tracking

Patch

Third Party Advisory

github.com

text/html

CONFIRM

github.com/radare/radare2/commit/d21e91f075a7a7a8ed23baa5c1bb1fac48313882

Crash in ELF version parse · Issue #8764 · radareorg/radare2 · GitHub

Exploit

Issue Tracking

Patch

Third Party Advisory

github.com

text/html

CONFIRM

github.com/radare/radare2/issues/8764

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	2.0.1	All	All	All
Application	Radare	Radare2	2.0.1	All	All	All

cpe:2.3:a:radare:radare2:2.0.1:****:****:

cpe:2.3:a:radare:radare2:2.0.1:****:****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →