



CVE-2019-16718

Published on: 09/23/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:49 PM UTC

CVE-2019-16718

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

In radare2 before 3.9.0, a command injection vulnerability exists in `bin_symbols()` in `lib/core/cbin.c`. By using a crafted executable file, it's possible to execute arbitrary shell commands with the permissions of the victim. This vulnerability is due to an insufficient fix for CVE-2019-14745 and improper handling of symbol names embedded in

executables.

CVE-2019-16718 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Comparing 3.8.0...3.9.0 · radareorg/radare2 · GitHub	Patch Third Party Advisory	MISC github.com/radareorg/radare2/compare/3.8.0...3.9.0

github.com
text/html

Fix #14990 - multiple quoted command parsing issue
##core ·
radareorg/radare2@dd739f5 · GitHub

Third Party Advisory
github.com
text/html

MISC
github.com/radareorg/radare2/commit/dd739f5a45b3af3d1f65f00fe19af1dbfec7aea7

Patch
Third Party Advisory
github.com
text/html

More fixes for the CVE-2019-14745 ·
radareorg/radare2@5411543 · GitHub

MISC
github.com/radareorg/radare2/commit/5411543a310a470b1257fb93273cdd6e8dfcb3af

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	All	All	All	All
Application	Radare	Radare2	All	All	All	All

cpe:2.3:a:radare:radare2:*****:.*

cpe:2.3:a:radare:radare2:*****:.*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →