

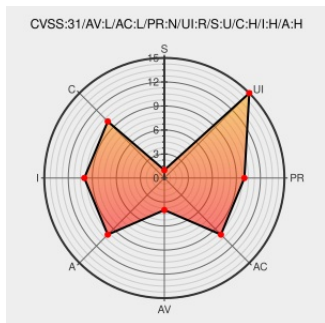


CVE-2019-19647

Published on: 12/08/2019 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:07:00 AM UTC

CVE-2019-19647

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

Certain versions of [Fedora](#) from [Fedoraproject](#) contain the following vulnerability:

radare2 through 4.0.0 lacks validation of the content variable in the function `r_asm_pseudo_incbin` at `libr/asm/asm.c`, ultimately leading to an arbitrary write. This allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted input.

CVE-2019-19647 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
Lack of Validation Check for `r_asm_pseudo_incbin` at `libr/asm/asm.c` · Issue #15545 · radareorg/radare2 · GitHub	Exploit Third Party Advisory github.com	MISC github.com/radareorg/radare2/issues/15545

[text/html](#)

[SECURITY] Fedora 31 Update: radare2-4.2.1-2.fc31 - package-announce - Fedora Mailing-Lists

lists.fedoraproject.org [FEDORA FEDORA-2020-acd8cdb08d](#)[text/html](#)

[SECURITY] Fedora 30 Update: cutter-re-1.10.1-3.fc30 - package-announce - Fedora Mailing-Lists

lists.fedoraproject.org [FEDORA FEDORA-2020-4a3ff78ba5](#)[text/html](#)

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.

Related QID Numbers

[503245](#) Alpine Linux Security Update for radare2

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Application	Radare	Radare2	All	All	All	All
cpe:2.3:o:fedoraproject:fedora:30:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:31:*:*:*:*:*:						
cpe:2.3:a:radare:radare2:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)