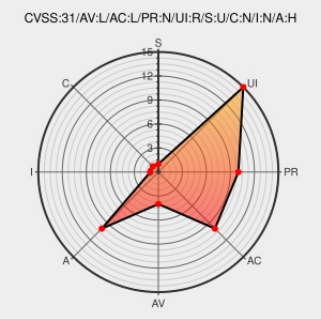
CVE-2021-32613

Published on: 05/14/2021 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:35:00 AM UTC

CVE-2021-32613

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



Certain versions of Fedora from Fedoraproject contain the following vulnerability:

In radare2 through 5.3.0 there is a double free vulnerability in the pyc parse via a crafted file which can lead to DoS.

CVE-2021-32613 has been assigned by patrick@puiterwijk.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
[SECURITY] Fedora 33 Update: iaito-5.2.2-3.fc33 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-ca59eb65a9

Fix #18666 - uaf in python bin parser · radareorg/radare2@5e16e2d · GitHub	github.com text/html	MISC github.com/radareorg/radare2/commit/5e16e2d1c9fe245e4c17005d779fde91ec0b9c05
Heap-use-after-free bug on .pyc parser · Issue #18666 · radareorg/radare2 · GitHub	github.com text/html	MISC github.com/radareorg/radare2/issues/18666
1959939 – (CVE-2021-32613) CVE-2021-32613 radare2: double free in pyc parse via creafted file	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1959939
[SECURITY] Fedora 34 Update: iaito-5.2.2-3.fc34 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-834f900f53
Heap memory bugs on pyc parse · Issue #18679 · radareorg/radare2 · GitHub	github.com text/html	MISC github.com/radareorg/radare2/issues/18679
Floating point exception on Mach-O parser · Issue #18667 · radareorg/radare2 · GitHub	github.com text/html	MISC github.com/radareorg/radare2/issues/18667
Fix #18667 - division by zero in the macho parser ##bin · radareorg/radare2@a07dedb · GitHub	github.com text/html	MISC github.com/radareorg/radare2/commit/a07dedb804a82bc01c07072861942dd80c6b6d6

Related QID Numbers

281649 Fedora Security Update for iaito (FEDORA-2021-834f900f53)

281650 Fedora Security Update for iaito (FEDORA-2021-ca59eb65a9)

503248 Alpine Linux Security Update for radare2

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Application	Radare	Radare2	All	All	All	All

cpe:2.3:o:fedoraproject:fedora:33:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:34:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-32613 : In radare2 through 5.3.0 there is a double free vulnerability in the pyc parse via a crafted file… twitter.com/i/web/status/1…	2021-05-14 13:04:59
/r/netcve	CVE-2021-32613	2021-05-14 13:41:55

← Previous ID

Next ID→