

Bug 2047923 (CVE-2022-25310) - CVE-2022-25310 fribidi: SEGV in fribidi_remove_bidi_marks

Keywords: Security x

Status: NEW

Alias: CVE-2022-25310

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: low

Severity: low

Target ---
Milestone:

Assignee: Red Hat Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Duplicates (1): [2047898](#) (view as bug list)

Depends On: [2050062](#) [2050063](#) [2067045](#)
[2067046](#)

Blocks: [2047924](#)

TreeView+ [depends on](#) / [blocked](#)

Reported: 2022-01-28 21:05 UTC by Pedro Sampaio

Modified: 2022-11-15 09:57 UTC ([History](#))

CC List: 15 users ([show](#))

Fixed In Version:

Doc Type: If docs needed, set a value

Doc Text: A segmentation fault (SEGV) flaw was found in the Fribidi package and affects the fribidi_remove_bidi_marks() function of the lib/fribidi.c file. This flaw allows an attacker to pass a specially crafted file to Fribidi, leading to a crash and causing a denial of service.

Clone Of:

Environment:

Last Closed:

Attachments	(Terms of Use)
Add an attachment (proposed patch, testcase, etc.)	

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2022:7514	0	None	None	None	2022-11-08 09:22:23 UTC
Red Hat Product Errata	RHSA-2022:8011	0	None	None	None	2022-11-15 09:57:52 UTC

Pedro Sampaio 2022-01-28 21:05:36 UTC

Description

SEGV found in fribidi_remove_bidi_marks.

References:

<https://github.com/fribidi/fribidi/issues/183>

TEJ RATHI 2022-03-23 06:13:23 UTC

Comment 6

Created fribidi tracking bugs for this issue:

Affects: fedora-all [[bug-2067045](#)]

Created mingw-fribidi tracking bugs for this issue:

Affects: fedora-all [[bug-2067046](#)]

TEJ RATHI 2022-05-10 08:10:20 UTC

Comment 7

*** [Bug-2047898](#) has been marked as a duplicate of this bug.

errata-xmlrpc 2022-11-08 09:22:21 UTC

Comment 8

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2022:7514 <https://access.redhat.com/errata/RHSA-2022:7514>

errata-xmlrpc 2022-11-15 09:57:50 UTC

Comment 9

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2022:8011 <https://access.redhat.com/errata/RHSA-2022:8011>

Note

You need to [log in](#) before you can comment on or make changes to this bug.

