Bug 2047896 (CVE-2022-25309) - CVE-2022-25309 fribidi: Heap-buffer-overflow in fribidi_cap_rtl_to_unicode

Keywords: Security ×

Status: NEW

Alias: CVE-2022-25309

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Red Hat Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 2050068 2050069 ~~2067042~~ ~~2067043~~

Blocks: 2047924

TreeView+ depends on / blocked

Reported: 2022-01-28 19:57 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 heap-based buffer overflow flaw was found in the Fribidi package and affects the fribidi_cap_rtl_to_unicode() function of the fribidi-char-sets-cap-rtl.c file. This flaw allows an attacker to pass a specially crafted file to the Fribidi application with the '--caprtl' option, 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 09:22:19 UTC
Red Hat Product Errata	RHSA-2022:8011	0	None	None	None	2022-11-15 09:57:50 UTC

Pedro Sampaio 2022-01-28 19:57:29 UTC Description

A heap based buffer overflow was found in fribidi_cap_rtl_to_unicode.

References:

https://github.com/fribidi/fribidi/issues/182

TEJ RATHI 2022-03-23 06:12:52 UTC Comment 6

Created fribidi tracking bugs for this issue:

Affects: fedora-all [~~bug 2067043~~]

Created mingw-fribidi tracking bugs for this issue:

Affects: fedora-all [~~bug 2067042~~]

errata-xmlrpc 2022-11-08 09:22:18 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 09:57:47 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.