

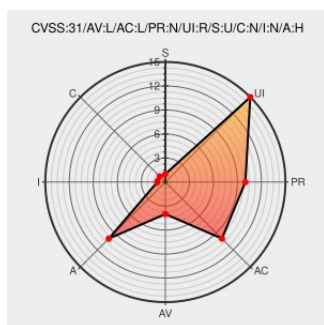


CVE-2022-25309

Published on: Not Yet Published

Last Modified on: 02/12/2023 10:15:00 PM UTC

CVE-2022-25309

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

Certain versions of [Fribidi](#) from [Gnu](#) contain the following vulnerability:

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.

CVE-2022-25309 has been assigned by [secalert@redhat.com](#) 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

CVE References

Description	Tags	Link
Protected against garbage in the CapRTL encoder · fribidi/fribidi@f22593b · GitHub	github.com text/html	MISC github.com/fribidi/fribidi/commit/f22593b82b5d1668d1997dbccd10a9c31ffea3b3
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2022:7514
heap-buffer-overflow (/home/lin/fribidi/bin/fribidi+0x108fe) in fribidi_cap_rtl_to_unicode · Issue #182 · fribidi/fribidi · GitHub	github.com text/html	MISC github.com/fribidi/fribidi/issues/182
2047896 – (CVE-2022-25309) CVE-2022-25309 fribidi: Heap-buffer-overflow in fribidi_cap_rtl_to_unicode	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=2047896

Red Hat Customer Portal - Access
to 24x7 support and knowledge

access.redhat.com
[text/html](#)

 [MISC access.redhat.com/errata/RHSA-2022:8011](https://access.redhat.com/errata/RHSA-2022:8011)

Red Hat Customer Portal - Access
to 24x7 support and knowledge

access.redhat.com
[text/html](#)

 [MISC access.redhat.com/security/cve/CVE-2022-25309](https://access.redhat.com/security/cve/CVE-2022-25309)

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

[160240](#) Oracle Enterprise Linux Security Update for fribidi (ELSA-2022-7514)

[160304](#) Oracle Enterprise Linux Security Update for fribidi (ELSA-2022-8011)

[179191](#) Debian Security Update for fribidi (DLA 2974-1)

[180868](#) Debian Security Update for fribidi (CVE-2022-25309)

[198732](#) Ubuntu Security Notification for FriBidi Vulnerabilities (USN-5366-1)

[198768](#) Ubuntu Security Notification for FriBidi Vulnerabilities (USN-5366-2)

[199483](#) Ubuntu Security Notification for FriBidi Vulnerabilities (USN-5922-1)

[240825](#) Red Hat Update for fribidi (RHSA-2022:7514)

[240871](#) Red Hat Update for fribidi (RHSA-2022:8011)

[282560](#) Fedora Security Update for mingw (FEDORA-2022-8c2af4ba24)

[282561](#) Fedora Security Update for mingw (FEDORA-2022-56942dc7c5)

[282563](#) Fedora Security Update for fribidi (FEDORA-2022-d230620a58)

[282595](#) Fedora Security Update for fribidi (FEDORA-2022-764c8c6b1c)

[354393](#) Amazon Linux Security Advisory for fribidi : ALAS2022-2022-200

[354444](#) Amazon Linux Security Advisory for fribidi : ALAS2022-2022-091

[355114](#) Amazon Linux Security Advisory for fribidi : ALAS2023-2023-069

[355326](#) Amazon Linux Security Advisory for fribidi : ALAS2-2023-2054

[502218](#) Alpine Linux Security Update for fribidi

[672347](#) EulerOS Security Update for fribidi (EulerOS-SA-2022-2763)

[672392](#) EulerOS Security Update for fribidi (EulerOS-SA-2022-2728)

[672430](#) EulerOS Security Update for fribidi (EulerOS-SA-2022-2820)

[672436](#) EulerOS Security Update for fribidi (EulerOS-SA-2022-2845)

[752174](#) SUSE Enterprise Linux Security Update for fribidi (SUSE-SU-2022:1845-1)

[752178](#) SUSE Enterprise Linux Security Update for fribidi (SUSE-SU-2022:1844-1)

[752194](#) SUSE Enterprise Linux Security Update for fribidi (SUSE-SU-2022:1898-1)

[752213](#) SUSE Enterprise Linux Security Update for fribidi (SUSE-SU-2022:2029-1)

903872 Common Base Linux Mariner (CBL-Mariner) Security Update for fribidi (10887-1)

903872 Common Base Linux Mariner (CBL-Mariner) Security Update for fribidi (10887)

904166 Common Base Linux Mariner (CBL-Mariner) Security Update for fribidi (10887-1)

940763 AlmaLinux Security Update for fribidi (ALSA-2022:7514)

940825 AlmaLinux Security Update for fribidi (ALSA-2022:8011)

960210 Rocky Linux Security Update for fribidi (RLSA-2022:7514)

960602 Rocky Linux Security Update for fribidi (RLSA-2022:8011)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Fribidi	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
cpe:2.3:a:gnu:fribidi:*:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux:8.0:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux:9.0:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 @CVereport	CVE-2022-25309 : A heap-based buffer overflow flaw was found in the Fribidi package and affects the fribidi_cap_rtl... twitter.com/i/web/status/1...	2022-09-06 18:22:30