



CVE-2022-25308

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-25308
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-06 18:15:00 UTC
Updated	2023-02-12 22:15:00 UTC
Description	A stack-based buffer overflow flaw was found in the Fribidi package. This flaw allows an attacker to pass a specially crafted

Risk And Classification

Problem Types: CWE-121

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference

Red Hat Customer Portal - Access to 24x7 support and knowledge
Fix the stack buffer overflow issue by tagoh · Pull Request #184 · fribidi/fribidi · GitHub
Red Hat Customer Portal - Access to 24x7 support and knowledge
stack-buffer-overflow on address 0x7ffda2c0112f at pc 0x5580929d7ab5 bp 0x7ffda2bc1820 sp 0x7ffda2bc1810 · Issue #181 · fribidi/fribidi · GitHub
Red Hat Customer Portal - Access to 24x7 support and knowledge
2047890 – (CVE-2022-25308) CVE-2022-25308 fribidi: Stack based buffer overflow
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[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)

[180828](#) Debian Security Update for fribidi (CVE-2022-25308)

[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

[355579](#) Amazon Linux Security Advisory for fribidi : ALAS2-2023-2116

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

[503933](#) 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)

[903836](#) Common Base Linux Mariner (CBL-Mariner) Security Update for fribidi (10854)

904157 Common Base Linux Mariner (CBL-Mariner) Security Update for fribidi (10854-1)
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)

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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