



# CVE-2022-27405

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

## Summary

<b>CVE</b>	CVE-2022-27405
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-04-22 14:15:00 UTC
<b>Updated</b>	2023-11-07 03:45:00 UTC
<b>Description</b>	FreeType commit 53dfdc8198d2b3201a23c4bad9190519ba918db was discovered to contain a segmentation violation via

## Risk And Classification

### Problem Types: CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Application	<a href="#">Freetype</a>	<a href="#">Freetype</a>	All	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 36 Update: mingw-freetype-2.12.1-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 35 Update: freetype-2.11.0-6.fc35 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 34 Update: freetype-2.10.4-6.fc34 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 36 Update: freetype-2.12.1-1.fc36 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 35 Update: freetype-2.11.0-6.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 36 Update: freetype-2.12.1-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
SEGV on FT_Set_Char_Size (#1139) · Issues · FreeType / FreeType · GitLab	MISC	<a href="#">gitlab.freedesktop.org</a>
[SECURITY] Fedora 35 Update: mingw-freetype-2.11.0-2.fc35 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 36 Update: mingw-freetype-2.12.1-1.fc36 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 34 Update: freetype-2.10.4-6.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>

Fonts.com   Find, Buy & Download Best Fonts	MISC	<a href="https://freetype.com">freetype.com</a>
[SECURITY] Fedora 35 Update: mingw-freetype-2.11.0-2.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[160215](#) Oracle Enterprise Linux Security Update for freetype (ELSA-2022-7745)

[160280](#) Oracle Enterprise Linux Security Update for freetype (ELSA-2022-8340)

[180880](#) Debian Security Update for freetype (CVE-2022-27405)

[198869](#) Ubuntu Security Notification for FreeType Vulnerabilities (USN-5528-1)

[240834](#) Red Hat Update for freetype (RHSA-2022:7745)

[240867](#) Red Hat Update for freetype (RHSA-2022:8340)

[242743](#) Red Hat Update for freetype (RHSA-2024:0420)

[282659](#) Fedora Security Update for mingw (FEDORA-2022-0985b0cb9f)

[282716](#) Fedora Security Update for mingw (FEDORA-2022-7ece4f6d74)

[282719](#) Fedora Security Update for freetype (FEDORA-2022-2dd60f1f00)

[282742](#) Fedora Security Update for freetype (FEDORA-2022-5e45671294)

[282743](#) Fedora Security Update for freetype (FEDORA-2022-80e1724780)

[354399](#) Amazon Linux Security Advisory for freetype : ALAS2022-2022-154

[354417](#) Amazon Linux Security Advisory for freetype : ALAS2022-2022-238

[354569](#) Amazon Linux Security Advisory for freetype : ALAS-2022-238

[354657](#) Amazon Linux Security Advisory for freetype : ALAS2-2023-1909

[355187](#) Amazon Linux Security Advisory for freetype : ALAS2023-2023-074

[355420](#) Amazon Linux Security Advisory for freetype : ALAS2023-2023-188

[500190](#) Alpine Linux Security Update for freetype

[501405](#) Alpine Linux Security Update for freetype

[501959](#) Alpine Linux Security Update for freetype

[502439](#) Alpine Linux Security Update for freetype

502485 Alpine Linux Security Update for qt5-qtwebengine
502946 Alpine Linux Security Update for qt5-qtwebengine
503930 Alpine Linux Security Update for freetype
505816 Alpine Linux Security Update for qt5-qtwebengine
610502 Google Android August 2023 Security Patch Missing for Huawei EMUI
610504 Google Android Devices July 2023 Security Patch Missing
671885 EulerOS Security Update for freetype (EulerOS-SA-2022-1928)
671922 EulerOS Security Update for freetype (EulerOS-SA-2022-1994)
671940 EulerOS Security Update for freetype (EulerOS-SA-2022-1964)
671985 EulerOS Security Update for freetype (EulerOS-SA-2022-2155)
671994 EulerOS Security Update for freetype (EulerOS-SA-2022-2130)
710854 Gentoo Linux FreeType Multiple Vulnerabilities (GLSA 202402-06)
752575 SUSE Enterprise Linux Security Update for freetype2 (SUSE-SU-2022:3252-1)
752605 SUSE Enterprise Linux Security Update for freetype2 (SUSE-SU-2022:3252-2)
901296 Common Base Linux Mariner (CBL-Mariner) Security Update for freetype (9612)
901551 Common Base Linux Mariner (CBL-Mariner) Security Update for freetype (9580)
903730 Common Base Linux Mariner (CBL-Mariner) Security Update for freetype (9612-1)
903859 Common Base Linux Mariner (CBL-Mariner) Security Update for freetype (9580-1)
940746 AlmaLinux Security Update for freetype (ALSA-2022:7745)
940791 AlmaLinux Security Update for freetype (ALSA-2022:8340)
960179 Rocky Linux Security Update for freetype (RLSA-2022:7745)
960605 Rocky Linux Security Update for freetype (RLSA-2022:8340)

© 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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**