



CVE-2026-34085

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

Summary

CVE	CVE-2026-34085
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-25 17:17:09 UTC
Updated	2026-05-12 15:37:22 UTC
Description	fontconfig before 2.17.1 has an off-by-one error in allocation during sfont capability handling, leading to a one-byte out-of-bo

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

CVSS: 3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.000140000 probability, percentile 0.028310000 (date 2026-05-12)

Problem Types: CWE-193 | CWE-193 CWE-193 Off-by-one Error

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	cve@mitre.org	Secondary	5.9	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	CVSS	5.9	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fontconfig Project	Fontconfig	2.17.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Fontconfig Project	Fontconfig	affected 2.17.1 semver	Not specified

References

Reference	Source	Link	Tags
gitlab.freedesktop.org/fontconfig/fontconfig/-/work_items/481	cve@mitre.org	gitlab.freedesktop.org	Issue
gitlab.freedesktop.org/fontconfig/fontconfig/-/merge_requests/446	cve@mitre.org	gitlab.freedesktop.org	Patch
gitlab.freedesktop.org/fontconfig/fontconfig/-/commit/b9bec06d73340f1b5727302d13ac3d...	cve@mitre.org	gitlab.freedesktop.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© 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