



CVE-2018-19876

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

Summary

CVE	CVE-2018-19876
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-12-05 20:29:00 UTC
Updated	2019-01-31 19:27:00 UTC
Description	cairo 1.16.0, in cairo_ft_apply_variations() in cairo-ft-font.c, would free memory using a free function incompatible with Web

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cairographics	Cairo	1.16.0	All	All	All
Application	Cairographics	Cairo	1.16.0	All	All	All

References

Reference	Source
ft: Use FT_Done_MM_Var instead of free when available in cairo_ft_apply_variations (15) · Merge Requests · cairo / cairo · GitLab	MISC
191595 – [FreeType] Problem under WebCore::FontPlatformData::FontPlatformData	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[500087](#) Alpine Linux Security Update for cairo

[503760](#) Alpine Linux Security Update for cairo

[900196](#) CBL-Mariner Linux Security Update for cairo 1.16.0

© [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](#)