



CVE-2017-14731

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

Summary

CVE	CVE-2017-14731
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-25 21:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	ofx_proc_file in ofx_preproc.cpp in LibOFX 0.9.12 allows remote attackers to cause a denial of service (heap-based buffer c

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libofx Project	Libofx	0.9.12	All	All	All
Application	Libofx Project	Libofx	0.9.12	All	All	All

References

Reference
libofx: Multiple vulnerabilities (GLSA 201908-26) — Gentoo security
CVE-2017-14731: ofxdump heap-buffer-overflow /usr/include/c++/4.9/bits/char_traits.h:263 std::char_traits<char>::length(char const*) · Issue
[SECURITY] [DLA 1192-1] libofx security update
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710135 Gentoo Linux libofx Multiple vulnerabilities (GLSA 201908-26)

© [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](#)