



CVE-2017-7378

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

Summary

CVE	CVE-2017-7378
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-03 05:59:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	The PoDoFo::PdfPainter::ExpandTabs function in PdfPainter.cpp in PoDoFo 0.9.5 allows remote attackers to cause a denial of service (CPU consumption) via a crafted PDF file.

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Podofo Project	Podofo	0.9.5	All	All	All
Application	Podofo Project	Podofo	0.9.5	All	All	All

References

Reference	Source	Link
podofo: heap-based buffer overflow in PoDoFo::PdfPainter::ExpandTabs (PdfPainter.cpp) agostino's blog	MISC	blogs.gentoo.org
podofo Null Pointer Dereference Denial of Service and Heap Based Buffer Overflow Vulnerabilities	BID	www.securityfocus.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[501671](#) Alpine Linux Security Update for podofo

[505251](#) Alpine Linux Security Update for podofo

© [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](#)