



CVE-2017-7994

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

Summary

CVE	CVE-2017-7994
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-21 16:59:00 UTC
Updated	2019-03-18 15:44:00 UTC
Description	The function TextExtractor::ExtractText in TextExtractor.cpp:77 in PoDoFo 0.9.5 allows remote attackers to cause a denial of service (memory consumption) via crafted PDF documents.

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
podofilter CVE-2017-7994 Denial of Service Vulnerability	BID	www.securityfocus.com	Third Party Advisory, VDB Entry
PoDoFo 0.9.5 NULL pointer dereference icepng's blog	MISC	icepng.github.io	Exploit, Third Party Advisory
PoC/PoC1 at master · icepng/PoC · GitHub	MISC	github.com	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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

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

© [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](#)