

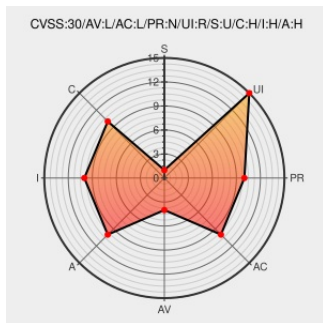


CVE-2017-6844

Published on: 03/15/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:50 PM UTC

CVE-2017-6844

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Podofo](#) from [Podofo Project](#) contain the following vulnerability:

Buffer overflow in the PoDoFo::PdfParser::ReadXRefSubsection function in PdfParser.cpp in PoDoFo 0.9.4 allows remote attackers to have unspecified impact via a crafted file.

CVE-2017-6844 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
podof: global buffer overflow in PoDoFo::PdfParser::ReadXRefSubsection (PdfParser.cpp) agostino's blog	Third Party Advisory VDB Entry blogs.gentoo.org text/html	MISC blogs.gentoo.org/ago/2017/03/02/podof-global-buffer-overflow-in-podofopdfparserreadxrefsubsection-pdfparser-cpp/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

501224 Alpine Linux Security Update for podof

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Podof Project	Podof	0.9.4	All	All	All
Application	Podof Project	Podof	0.9.4	All	All	All
cpe:2.3:a:podof_project:podof:0.9.4:*:*:*:*:*:						
cpe:2.3:a:podof_project:podof:0.9.4:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→