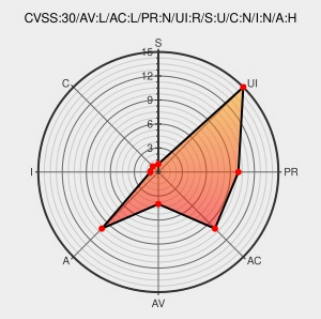
CVE-2017-6846

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

Last Modified on: 03/23/2021 11:26:49 PM UTC

CVE-2017-6846

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Podofo from Podofo Project contain the following vulnerability:

The GraphicsStack::TGraphicsStackElement::SetNonStrokingColorSpace function in graphicsstack.h in PoDoFo 0.9.4 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted file.

CVE-2017-6846 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
podofo: NULL pointer dereference in GraphicsStack::TGraphicsStackElement::SetNonStrokingColorSpace (graphicsstack.h) | agostino's blog	Third Party Advisory VDB Entry blogs.gentoo.org text/html	MISC blogs.gentoo.org/ago/2017/03/02/podc pointer-dereference-in-graphicsstacktgraphicsstackelementsetnonstrok graphicsstack-h/

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 podofo

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Podofo Project	Podofo	0.9.4	All	All	All
Application	Podofo Project	Podofo	0.9.4	All	All	All

cpe:2.3:a:podofo_project:podofo:0.9.4:*:*:*:*:*:*:*

cpe:2.3:a:podofo_project:podofo:0.9.4:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 | |
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 registred 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