



# CVE-2017-6840

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

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

## CVE-2017-6840

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

The `ColorChanger::GetColorFromStack` function in `colorchanger.cpp` in PoDoFo 0.9.5 allows remote attackers to cause a denial of service (invalid read) via a crafted file.

CVE-2017-6840 has been assigned by [M](#) [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                                                                                                                              |
|----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| podof: invalid memory read in ColorChanger::GetColorFromStack (colorchanger.cpp)   agostino's blog | <a href="#">Third Party Advisory</a><br><a href="#">VDB Entry</a><br><a href="#">blogs.gentoo.org</a><br><a href="#">text/html</a> | <a href="#">MISC blogs.gentoo.org/ago/2017/03/02/podof-invalid-memory-read-in-colorchangergetcolorfromstack-colorchanger-cpp/</a> |

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](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

| Type                                             | Vendor                         | Product                | Version | Update | Edition | Language |
|--------------------------------------------------|--------------------------------|------------------------|---------|--------|---------|----------|
| Application                                      | <a href="#">Podofo Project</a> | <a href="#">Podofo</a> | 0.9.5   | All    | All     | All      |
| Application                                      | <a href="#">Podofo Project</a> | <a href="#">Podofo</a> | 0.9.5   | All    | All     | All      |
| cpe:2.3:a:podofo_project:podofo:0.9.5:*:*:*:*:*: |                                |                        |         |        |         |          |
| cpe:2.3:a:podofo_project:podofo:0.9.5:*:*:*:*:*: |                                |                        |         |        |         |          |

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 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)