

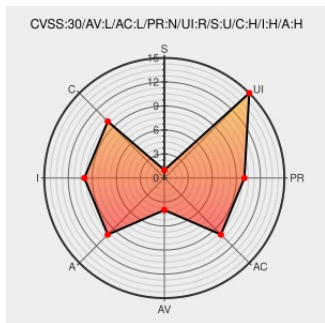


CVE-2017-14685

Published on: 09/22/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:44 PM UTC

CVE-2017-14685

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

Certain versions of [Mupdf](#) from [Artifex](#) contain the following vulnerability:

Artifex MuPDF 1.11 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .xps file, related to "Data from Faulting Address controls Branch Selection starting at mupdf+0x000000000016aa61" on Windows. This occurs because xps_load_links_in_glyphs in xps/xps-link.c does not verify that an xps

font could be loaded.

CVE-2017-14685 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
Page not found · GitHub · GitHub	Third Party Advisory github.com	MISC github.com/wlinzi/security_advisories/tree/master/CVE-2017-

	text/html Inactive Link Not Archived	14685
git.ghostscript.com Git - mupdf.git/commit	Patch git.ghostscript.com text/xml	MISC git.ghostscript.com/?p=mupdf.git;h=ab1a420613dec93c686acbee2c165274e922f82a
698539 – mupdf 1.11 windows allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .xps file, related to a "Data from Faulting Address controls Branch Selection starting at mupdf+0x000000000016aa61".	Exploit Third Party Advisory bugs.ghostscript.com text/html	MISC bugs.ghostscript.com/show_bug.cgi?id=698539
Debian -- Security Information -- DSA-4006-1 mupdf	www.debian.org Deprecated Link text/html	DEBIAN DSA-4006

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Artifex	Mupdf	1.11	All	All	All
Application	Artifex	Mupdf	1.11	All	All	All
Operating System	Microsoft	Windows	All	All	All	All
Operating System	Microsoft	Windows	All	All	All	All
cpe:2.3:a:artifex:mupdf:1.11:*****:*						
cpe:2.3:a:artifex:mupdf:1.11:*****:*						
cpe:2.3:o:microsoft:windows:*****:*						
cpe:2.3:o:microsoft:windows:*****:*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)