



CVE-2020-19609

Published on: 07/21/2021 12:00:00 AM UTC

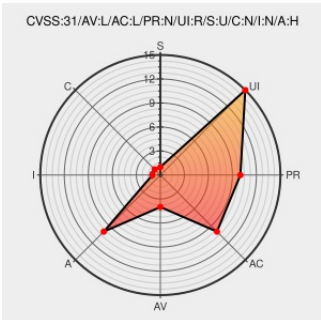
Last Modified on: 07/29/2021 07:21:00 PM UTC

CVE-2020-19609

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)



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

Artifex MuPDF before 1.18.0 has a heap based buffer over-write in `tiff_expand_colormap()` function when parsing TIFF files allowing attackers to cause a denial of service.

CVE-2020-19609 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
701176 – Integer overflow in source/fitz/load-tiff.c:272	bugs.ghostscript.com text/html	MISC bugs.ghostscript.com/show_bug.cgi?id=701176
git.ghostscript.com Git - mupdf.git/commit	git.ghostscript.com text/xml	MISC git.ghostscript.com/?p=mupdf.git;h=b7892cdc7fae62aa57d63ae62144e1f11b5f9275

703076 – Buffer Overflow in
tiff_expand_colormap() function in source/fitz/load-
tiff.c:256:25

bugs.ghostscript.com
text/html

 [MISC bugs.ghostscript.com/show_bug.cgi?id=703076](https://bugs.ghostscript.com/show_bug.cgi?id=703076)

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	All	All	All	All
cpe:2.3:a:artifex:mupdf:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2020-19609 : Artifex MuPDF before 1.18.0 has a heap based buffer over-write in tiff_expand_colormap function... twitter.com/i/web/status/1...	2021-07-21 15:09:26
 @WesUncensored	New vulnerability on the NVD: CVE-2020-19609 ift.tt/3eD7TZm	2021-07-21 16:48:19
 @Velletron	CVE-2020-19609 ift.tt/3eD7TZm #CVE #Vulnerability	2021-07-21 16:54:34
 @xanadulinux	CVE-2020-19609 ift.tt/3eD7TZm	2021-07-21 17:02:31
 @workentin	New vulnerability on the NVD: CVE-2020-19609 ift.tt/3eD7TZm	2021-07-21 17:05:38
 @threatmeter	CVE-2020-19609 Artifex MuPDF before 1.18.0 has a heap based buffer over-write in tiff_expand_colormap() function wh... twitter.com/i/web/status/1...	2021-07-22 07:09:33
 /r/netcve	CVE-2020-19609	2021-07-21 15:38:30

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2021   |

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](#).

