



CVE-2018-18662

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2018-18662
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-26 14:29:00 UTC
Updated	2020-07-26 00:15:00 UTC
Description	There is an out-of-bounds read in fz_run_t3_glyph in fitz/font.c in Artifex MuPDF 1.14.0, as demonstrated by mutool.

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Artifex	Mupdf	1.14.0	All	All	All
Application	Artifex	Mupdf	1.14.0	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] [DLA 2289-1] mupdf security update	MLIST	lists.debian.org	
Bug 700043 – there is a out-of-bound-read bug in font.c:1398	MISC	bugs.ghostscript.com	Exploit, Third Party Advisory
pocs/mupdf at master · TeamSerious/pocs · GitHub	MISC	github.com	Exploit, Third Party Advisory
Artifex MuPDF CVE-2018-18662 Denial of Service Vulnerability	BID	www.securityfocus.com	Third Party Advisory, VDB Entry
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report