CVE-2017-5896

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-5896
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-15 19:59:00 UTC
Updated	2023-11-07 02:49:00 UTC
Description	Heap-based buffer overflow in the fz_subsample_pixmap function in fitz/pixmap.c in MuPDF 1.10a allows remote attackers

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
git.ghostscript.com Git - mupdf.git/commit	CONFIRM	git.ghostscript.com	Issue Tracking, Patch
MuPDF 'fitz/pixmap.c' Heap Based Buffer Overflow Vulnerability	BID	www.securityfocus.com	Third Party Advisory,
git.ghostscript.com Git - mupdf.git/commit		git.ghostscript.com	
697515 – Heap out of bounds read in fz_subsample_pixmap()	CONFIRM	bugs.ghostscript.com	Issue Tracking, Patch
oss-security - Re: mupdf: heap-based buffer overflow in fz_subsample_pixmap	MLIST	www.openwall.com	Mailing List, Patch, T
MuPDF: Multiple vulnerabilities (GLSA 201702-12) — Gentoo Security	GENTOO	security.gentoo.org	
oss-security - mupdf: heap-based buffer overflow in fz_subsample_pixmap	MLIST	www.openwall.com	Mailing List, Patch, T
Debian -- Security Information -- DSA-3797-1 mupdf	DEBIAN	www.debian.org	
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.

Legacy QID Mappings

501082 Alpine Linux Security Update for mupdf

710497 Gentoo Linux MuPDF Multiple Vulnerabilities (GLSA 201702-12)

Free CVE JSON API cve.report/api

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