



CVE-2019-9877

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

Summary

CVE	CVE-2019-9877
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-21 16:01:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	There is an invalid memory access vulnerability in the function TextPage::findGaps() located at TextOutputDev.c in Xpdf 4.0.1. The vulnerability allows an attacker to cause a denial of service by sending a crafted PDF file to the application.

Risk And Classification

Problem Types: CWE-125 | CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xpdfreader	Xpdf	4.0.1	All	All	All
Application	Xpdfreader	Xpdf	4.0.1	All	All	All

References

Reference	Source	Link	Ta
invalid memory access in TextPage::findGaps() – xpdf-4.01 - forum.xpdfreader.com	MISC	forum.xpdfreader.com	Ve
CVE-2019-9877: Invalid memory access in TextPage::findGaps() - xpdf-4.01 - Loginsoft Research	MISC	research.loginsoft.com	Ex
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[690709](#) Free Berkeley Software Distribution (FreeBSD) Security Update for xpdf (791e8f79-e7d1-11e9-8b31-206a8a720317)

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](#)