



CVE-2017-7976

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

Summary

CVE	CVE-2017-7976
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-19 17:59:00 UTC
Updated	2017-11-04 01:29:00 UTC
Description	Artifex jbig2dec 0.13 allows out-of-bounds writes and reads because of an integer overflow in the jbig2_image_compose fu

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Artifex	Jbig2dec	0.13	All	All	All
Application	Artifex	Jbig2dec	0.13	All	All	All

References

Reference	Source	Link	Tags
jbig2dec: User-assisted execution of arbitrary code (GLSA 201708-10) — Gentoo Security	GENTOO	security.gentoo.org	
Bug 697683 – jbig2dec-0.13 Integer Overflow in function jbig2_image_compose	MISC	bugs.ghostscript.com	Issue Track
Debian -- Security Information -- DSA-3855-1 jbig2dec	DEBIAN	www.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[670288](#) EulerOS Security Update for ghostscript (EulerOS-SA-2021-1788)

[670614](#) EulerOS Security Update for ghostscript (EulerOS-SA-2021-2372)

[710510](#) CentOS Linux Security Update for ghostscript (CESA-2021-10)

© [CVE.report](#) 2026 |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)