



CVE-2016-7977

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

Summary

CVE	CVE-2016-7977
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-23 04:29:00 UTC
Updated	2023-11-07 02:35:00 UTC
Description	Ghostscript before 9.21 might allow remote attackers to bypass the SAFER mode protection mechanism and consequently

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
git.ghostscript.com Git - ghostpd.git/commitdiff	CONFIRM	git.ghostscript.com	Patch
697169 – .libfile does not honor -dSAFER	CONFIRM	bugs.ghostscript.com	Issue Tracking, F
git.ghostscript.com Git - ghostpd.git/commitdiff		git.ghostscript.com	
oss-security - Re: ImageMagick identify "d:" hangs	MLIST	www.openwall.com	Mailing List, Patc
oss-security - Re: CVE Request - multiple ghostscript -dSAFER sandbox problems	MLIST	www.openwall.com	Mailing List, Patc
Oracle Critical Patch Update - January 2018	CONFIRM	www.oracle.com	
Red Hat Customer Portal	REDHAT	rhn.redhat.com	
Red Hat Customer Portal	REDHAT	rhn.redhat.com	
Ghostscript CVE-2016-7977 Information Disclosure Vulnerability	BID	www.securityfocus.com	Third Party Advis
GPL Ghostscript: Multiple vulnerabilities (GLSA 201702-31) — Gentoo Security	GENTOO	security.gentoo.org	
History of Ghostscript versions 9.n	CONFIRM	ghostscript.com	Release Notes
Debian -- Security Information -- DSA-3691-1 ghostscript	DEBIAN	www.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[378143](#) Virtuozzo Linux Security Update for ghostscript-doc (VZLSA-2017:0013)

[378268](#) Virtuozzo Linux Security Update for ghostscript-devel (VZLSA-2017:0014)

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

[710453](#) Gentoo Linux GPL Ghostscript Multiple Vulnerabilities (GLSA 201702-31)

© [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](#)