



# CVE-2016-7979

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

## Summary

<b>CVE</b>	CVE-2016-7979
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-05-23 04:29:00 UTC
<b>Updated</b>	2023-11-07 02:35:00 UTC
<b>Description</b>	Ghostscript before 9.21 might allow remote attackers to bypass the SAFER mode protection mechanism and consequently

## Risk And Classification

**Problem Types:** CWE-704

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Artifex</a>	<a href="#">Ghostscript</a>	All	All	All	All

## References

Reference	Source	Link	Tags
git.ghostscript.com Git - ghostpdl.git/commit	CONFIRM	<a href="#">git.ghostscript.com</a>	Patch
oss-security - Re: CVE Request - multiple ghostscript -dSAFER sandbox problems	MLIST	<a href="#">www.openwall.com</a>	Mailing L
Red Hat Customer Portal	REDHAT	<a href="#">rhn.redhat.com</a>	
Red Hat Customer Portal	REDHAT	<a href="#">rhn.redhat.com</a>	
GPL Ghostscript: Multiple vulnerabilities (GLSA 201702-31) — Gentoo Security	GENTOO	<a href="#">security.gentoo.org</a>	
git.ghostscript.com Git - ghostpdl.git/commit		<a href="#">git.ghostscript.com</a>	
Ghostscript CVE-2016-7979 Remote Code Execution Vulnerability	BID	<a href="#">www.securityfocus.com</a>	Third Pa
Debian -- Security Information -- DSA-3691-1 ghostscript	DEBIAN	<a href="#">www.debian.org</a>	
697190 - .initialize_dsc_parser doesn't validate the parameter is a dict type before using it.	CONFIRM	<a href="#">bugs.ghostscript.com</a>	Issue Tra
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonica
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonica

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)

[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](#)