



CVE-2017-11714

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2017-11714
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-28 05:29:00 UTC
Updated	2023-11-07 02:38:00 UTC
Description	psi/ztoken.c in Artifex Ghostscript 9.21 mishandles references to the scanner state structure, which 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	Ghostscript	9.21	All	All	All
Application	Artifex	Ghostscript	9.21	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All

References

Reference

Ghostscript Double Free Memory Error in tokenexec_continue() Lets Remote Users Cause the Target Application to Crash - SecurityTracker
git.ghostscript.com Git - ghostpdl.git/commit
Debian -- Security Information -- DSA-3986-1 ghostscript
git.ghostscript.com Git - ghostpdl.git/commit
GPL Ghostscript: Multiple vulnerabilities (GLSA 201811-12) — Gentoo security
698158 – Ghostscript - Out of bounds read in igc_reloc_struct_ptr()
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[671112](#) EulerOS Security Update for ghostscript (EulerOS-SA-2019-2370)

[710304](#) Gentoo Linux GPL Ghostscript Multiple Vulnerabilities (GLSA 201811-12)

© [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](#)