CVE-2018-16802

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-16802
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-09-10 16:29:00 UTC
Updated	2023-11-07 02:53:00 UTC
Description	An issue was discovered in Artifex Ghostscript before 9.25. Incorrect "restoration of privilege" checking when running out of

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Artifex	Ghostscript	All	All	All	All
Application	Artifex	Ghostscript	All	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	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
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All

Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

References

Reference	Source	Link	Tags
git.ghostscript.com Git - ghostpdl.git/commit		git.ghostscript.com	
USN-3768-1: Ghostscript vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third F
git.ghostscript.com Git - ghostpdl.git/commitdiff		git.ghostscript.com	
git.ghostscript.com Git - ghostpdl.git/commit		git.ghostscript.com	
git.ghostscript.com Git - ghostpdl.git/commitdiff	CONFIRM	git.ghostscript.com	Patch,
Red Hat Customer Portal	REDHAT	access.redhat.com	Third F
oss-sec: Re: Re: More Ghostscript Issues: Should we disable PS coders in policy.xml by default?	MISC	seclists.org	Mailing
GPL Ghostscript: Multiple vulnerabilities (GLSA 201811-12) — Gentoo security	GENTOO	security.gentoo.org	Third F
git.ghostscript.com Git - ghostpdl.git/commit	MISC	git.ghostscript.com	Third F
Debian -- Security Information -- DSA-4294-1 ghostscript	DEBIAN	www.debian.org	Third F
oss-sec: Re: Ghostscript 9.24 issues	MLIST	seclists.org	Mailing
[SECURITY] [DLA 1504-1] ghostscript security update	MLIST	lists.debian.org	Mailing
git.ghostscript.com Git - ghostpdl.git/commit	MISC	git.ghostscript.com	Third F
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500207 Alpine Linux Security Update for ghostscript

503949 Alpine Linux Security Update for ghostscript

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 registred 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