



# CVE-2018-19477

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

## Summary

<b>CVE</b>	CVE-2018-19477
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-11-23 05:29:00 UTC
<b>Updated</b>	2023-11-07 02:55:00 UTC
<b>Description</b>	psi/zfjbig2.c in Artifex Ghostscript before 9.26 allows remote attackers to bypass intended access restrictions because of a

## 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
Application	<a href="#">Artifex</a>	<a href="#">Ghostscript</a>	All	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All

Operating System	Redhat	Enterprise Linux Server	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.6	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
Application	Redhat	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All

## References

Reference	Source	Link	Tags
git.ghostscript.com Git - ghostpdl.git/commit	MISC	<a href="https://git.ghostscript.com">git.ghostscript.com</a>	Patch, Vendor Advisory
History of Ghostscript versions 9.n	MISC	<a href="http://www.ghostscript.com">www.ghostscript.com</a>	Release Notes, Vendor A
[SECURITY] [DLA 1598-1] ghostscript security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>	Mailing List, Third Party A
git.ghostscript.com Git - ghostpdl.git/commit		<a href="https://git.ghostscript.com">git.ghostscript.com</a>	
Ghostscript Vulnerabilities in Postscript & PDF Processings   Semmler Blog	MISC	<a href="http://semmler.com">semmler.com</a>	Exploit, Mitigation, Third I
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
Access Denied	MISC	<a href="https://bugs.ghostscript.com">bugs.ghostscript.com</a>	Issue Tracking, Patch, Ve
Debian -- Security Information -- DSA-4346-1 ghostscript	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	Third Party Advisory
git.ghostscript.com Git - ghostpdl.git/commit		<a href="https://git.ghostscript.com">git.ghostscript.com</a>	
USN-3831-1: Ghostscript vulnerabilities   Ubuntu security notices	UBUNTU	<a href="http://usn.ubuntu.com">usn.ubuntu.com</a>	Third Party Advisory
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
git.ghostscript.com Git - ghostpdl.git/commit	MISC	<a href="https://git.ghostscript.com">git.ghostscript.com</a>	Patch, Vendor Advisory
Ghostscript Multiple Security Bypass Vulnerabilities	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Third Party Advisory, VDI
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[377191](#) Alibaba Cloud Linux Security Update for ghostscript (ALINUX2-SA-2019:0003)

[500209](#) Alpine Linux Security Update for ghostscript

[503951](#) Alpine Linux Security Update for ghostscript

© [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](#)**