



# CVE-2018-16542

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

## Summary

<b>CVE</b>	CVE-2018-16542
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-09-05 18:29:00 UTC
<b>Updated</b>	2023-11-07 02:53:00 UTC
<b>Description</b>	In Artifex Ghostscript before 9.24, attackers able to supply crafted PostScript files could use insufficient interpreter stack-siz

## Risk And Classification

**Problem Types:** CWE-787

## 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>	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="#">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</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</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 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	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All

## References

Reference	Source	Link	Tags
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Threat Intelligence
USN-3768-1: Ghostscript vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	Threat Intelligence
git.ghostscript.com Git - ghostpdl.git/commit		<a href="https://git.ghostscript.com">git.ghostscript.com</a>	
git.ghostscript.com Git - ghostpdl.git/commit	MISC	<a href="https://git.ghostscript.com">git.ghostscript.com</a>	Package
Ghostscript 'psi/interp.c' Remote Memory Corruption Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	Threat Intelligence
GPL Ghostscript: Multiple vulnerabilities (GLSA 201811-12) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	Threat Intelligence
Debian -- Security Information -- DSA-4288-1 ghostscript	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	Threat Intelligence
oss-sec: Re: Re: More Ghostscript Issues: Should we disable PS coders in policy.xml by default?	MISC	<a href="https://seclists.org">seclists.org</a>	Mail
699668 – .definemodifiedfont memory corruption if /typecheck is handled	MISC	<a href="https://bugs.ghostscript.com">bugs.ghostscript.com</a>	Issue
[SECURITY] [DLA 1504-1] ghostscript security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	Mail
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	Category
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	Category

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[378172](#) Virtuozzo Linux Security Update for ghostscript-doc (VZLSA-2018:2918)

[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](https://status.cve.report)