



# CVE-2018-16513

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

## Summary

<b>CVE</b>	CVE-2018-16513
<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 13:29:00 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 a type confusion in the setcolor

## 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
Application	<a href="#">Artifex</a>	<a href="#">Gpl Ghostscript</a>	All	All	All	All
Application	<a href="#">Artifex</a>	<a href="#">Gpl 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
Application	<a href="#">Pulsesecure</a>	<a href="#">Pulse Connect Secure</a>	All	All	All	All
Application	<a href="#">Pulsesecure</a>	<a href="#">Pulse Connect Secure</a>	All	All	All	All

## References

### Reference

USN-3768-1: Ghostscript vulnerabilities | Ubuntu security notices

699655 – missing type checking in setcolor

myF5

git.ghostscript.com Git - ghostpd.git/commit

Ghostscript security vulnerabilities resolved | Artifex

Public KB - SA44101 - 2019-04: Out-of-Cycle Advisory: Multiple vulnerabilities resolved in Pulse Connect Secure / Pulse Policy Secure 9.0RX

GPL Ghostscript: Multiple vulnerabilities (GLSA 201811-12) — Gentoo security

Debian -- Security Information -- DSA-4288-1 ghostscript

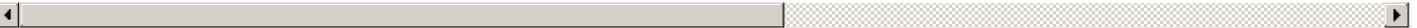
support.f5.com/csp/article/K22141757

git.ghostscript.com Git - ghostpd.git/commit

[SECURITY] [DLA 1504-1] ghostscript security update

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[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](#)