



CVE-2018-15909

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

Summary

CVE	CVE-2018-15909
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-27 17:29:00 UTC
Updated	2023-11-07 02:53:00 UTC
Description	In Artifex Ghostscript 9.23 before 2018-08-24, a type confusion using the .shfill operator could be used by attackers able to

Risk And Classification

Problem Types: CWE-704

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Artifex	Ghostscript	All	All	All	All
Application	Artifex	Gpl Ghostscript	All	All	All	All
Application	Artifex	Gpl 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	8.0	All	All	All
Application	Pulsesecure	Pulse Connect Secure	All	All	All	All
Application	Pulsesecure	Pulse Connect Secure	All	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

[USN-3768-1: Ghostscript vulnerabilities | Ubuntu security notices](#)

[git.ghostscript.com Git - ghostpdl.git/commit](#)

[Red Hat Customer Portal](#)

[CERT Vulnerability Notes Database](#)

[git.ghostscript.com Git - ghostpdl.git/commit](#)

[support.f5.com/csp/article/K24803507](#)

[git.ghostscript.com Git - ghostpdl.git/commit](#)

[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](#)

[Ghostscript 'shading_param' Remote Code Execution Vulnerability](#)

[git.ghostscript.com Git - ghostpdl.git/commit](#)

[myF5](#)

[\[SECURITY\] \[DLA 1504-1\] ghostscript security update](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[296090](#) Oracle Solaris 11.4 Support Repository Update (SRU) 5.1.3 Missing (CPUJAN2019)

[500206](#) Alpine Linux Security Update for ghostscript

[503948](#) 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 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](#)