



CVE-2019-14811

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

Summary

CVE	CVE-2019-14811
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-09-03 16:15:00 UTC
Updated	2023-11-07 03:05:00 UTC
Description	A flaw was found in, ghostscript versions prior to 9.50, in the .pdf_hook_DSC_Creator procedure where it did not properly s

Risk And Classification

Problem Types: CWE-863

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	Debian	Debian Linux	10.0	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	Debian	Debian Linux	10.0	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	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All

Operating System	Opensuse	Leap	15.1	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Openshift Container Platform	4.1	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Openshift Container Platform	4.1	All	All	All

References

Reference

Bugtraq: [SECURITY] [DSA 4518-1] ghostscript security update

[SECURITY] Fedora 29 Update: ghostscript-9.27-1.fc29 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 31 Update: ghostscript-9.27-1.fc31 - package-announce - Fedora Mailing-Lists

Debian -- Security Information -- DSA-4518-1 ghostscript

[SECURITY] Fedora 29 Update: ghostscript-9.27-1.fc29 - package-announce - Fedora Mailing-Lists

Red Hat Customer Portal

[SECURITY] [DLA 1915-1] ghostscript security update

[SECURITY] Fedora 30 Update: ghostscript-9.27-1.fc30 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 31 Update: ghostscript-9.27-1.fc31 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 30 Update: ghostscript-9.27-1.fc30 - package-announce - Fedora Mailing-Lists

GPL Ghostscript: Multiple vulnerabilities (GLSA 202004-03) — Gentoo security

[security-announce] openSUSE-SU-2019:2222-1: important: Security update

[security-announce] openSUSE-SU-2019:2223-1: important: Security update

Red Hat Customer Portal

1743757 – (CVE-2019-14811) CVE-2019-14811 ghostscript: Safer mode bypass by .forceput exposure in .pdf_hook_DSC_Creator (701445)

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[296079](#) Oracle Solaris 11.4 Support Repository Update (SRU) 15.5.0 Missing (CPUOCT2019)

[377082](#) Alibaba Cloud Linux Security Update for ghostscript (ALINUX2-SA-2019:0098)

[377128](#) Alibaba Cloud Linux Security Update for ghostscript (ALINUX3-SA-2022:0123)

[378191](#) Virtuozzo Linux Security Update for libgs-devel (VZLSA-2019:2586)

[500212](#) 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](#)