



# CVE-2019-14813

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

## Summary

<b>CVE</b>	CVE-2019-14813
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-09-06 14:15:00 UTC
<b>Updated</b>	2023-11-07 03:05:00 UTC
<b>Description</b>	A flaw was found in ghostscript, versions 9.x before 9.50, in the setsystemparams procedure where it did not properly secu

## Risk And Classification

**Problem Types:** CWE-863

## 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
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	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="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	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="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All

Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	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	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	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	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	Source
Bugtraq: [SECURITY] [DSA 4518-1] ghostscript security update	BUGTRAQ
[SECURITY] Fedora 29 Update: ghostscript-9.27-1.fc29 - package-announce - Fedora Mailing-Lists	FEDORA
[SECURITY] Fedora 31 Update: ghostscript-9.27-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA
Debian -- Security Information -- DSA-4518-1 ghostscript	DEBIAN
git.ghostscript.com Git - ghostpdl.git/commitdiff	CONTRIBUTORS
[SECURITY] Fedora 29 Update: ghostscript-9.27-1.fc29 - package-announce - Fedora Mailing-Lists	FEDORA
Red Hat Customer Portal	RED HAT
[SECURITY] [DLA 1915-1] ghostscript security update	MLIS
[SECURITY] Fedora 30 Update: ghostscript-9.27-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA
[SECURITY] Fedora 31 Update: ghostscript-9.27-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA
git.ghostscript.com Git - ghostpdl.git/commitdiff	CONTRIBUTORS
1743737 – (CVE-2019-14813) CVE-2019-14813 ghostscript: Safer mode bypass by .forceput exposure in setsystemparams (701443)	CONTRIBUTORS
[SECURITY] Fedora 30 Update: ghostscript-9.27-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA

[SECURITY] Fedora 30 Update: ghostscript-9.27-1.fc30 - package-announce - Fedora Mailing-Lists	FEDU
GPL Ghostscript: Multiple vulnerabilities (GLSA 202004-03) — Gentoo security	GEN
[security-announce] openSUSE-SU-2019:2222-1: important: Security update	SUSE
[security-announce] openSUSE-SU-2019:2223-1: important: Security update	SUSE
Red Hat Customer Portal	REDH
CVE Program record	CVE.
NVD vulnerability detail	NVD

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

[503955](#) 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](#)