



CVE-2019-14869

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

Summary

CVE	CVE-2019-14869
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-11-15 12:15:00 UTC
Updated	2023-11-07 03:05:00 UTC
Description	A flaw was found in all versions of ghostscript 9.x before 9.50, where the <code>`.charkeys`</code> procedure, where it did not properly se

Risk And Classification

Problem Types: CWE-732

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	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

References

Reference	Source	Link
Bugtraq: [SECURITY] [DSA 4569-1] ghostscript security update	BUGTRAQ	seclists.org
[SECURITY] Fedora 30 Update: ghostscript-9.27-2.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org

oss-security - CVE-2019-14869 ghostscript: -dSAFER escape in .charkeys	MLIST	www.openwall.com
[SECURITY] Fedora 29 Update: ghostscript-9.27-2.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
Bug Access Denied	CONFIRM	bugs.ghostscript.com
Red Hat Customer Portal	REDHAT	access.redhat.com
[SECURITY] Fedora 29 Update: ghostscript-9.27-2.fc29 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
git.ghostscript.com Git - ghostpdl.git/commitdiff	CONFIRM	git.ghostscript.com
[SECURITY] Fedora 31 Update: ghostscript-9.27-2.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
git.ghostscript.com Git - ghostpdl.git/commitdiff		git.ghostscript.com
[security-announce] openSUSE-SU-2019:2535-1: important: Security update	SUSE	lists.opensuse.org
JVN#52486659: Ghostscript access restriction bypass vulnerability	JVN	jvn.jp
[security-announce] openSUSE-SU-2019:2534-1: important: Security update	SUSE	lists.opensuse.org
1768911 – (CVE-2019-14869) CVE-2019-14869 ghostscript: -dSAFER escape in .charkeys (701841)	CONFIRM	bugzilla.redhat.com
[SECURITY] Fedora 30 Update: ghostscript-9.27-2.fc30 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 31 Update: ghostscript-9.27-2.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[296071](#) Oracle Solaris 11.4 Support Repository Update (SRU) 27.82.1 Missing (CPUOCT2020)

[376898](#) Alibaba Cloud Linux Security Update for ghostscript (ALINUX2-SA-2020:0001)

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

[378272](#) Virtuozzo Linux Security Update for ghostscript-cups (VZLSA-2019:3888)

[500214](#) Alpine Linux Security Update for ghostscript

[503957](#) 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