



# CVE-2019-3835

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

## Summary

<b>CVE</b>	CVE-2019-3835
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-03-25 19:29:00 UTC
<b>Updated</b>	2023-11-07 03:10:00 UTC
<b>Description</b>	It was found that the superexec operator was available in the internal dictionary in ghostscript before 9.27. A specially crafted

## Risk And Classification

**Problem Types:** CWE-862

## 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
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
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	28	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>	28	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="#">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
Application	<a href="#">Redhat</a>	<a href="#">Ansible Tower</a>	3.3	All	All	All

Application	<a href="#">Redhat</a>	<a href="#">Ansible Tower</a>	3.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All

## References

Reference	Source	Link
Bugtraq: [SECURITY] [DSA 4432-1] ghostscript security update	BUGTRAQ	<a href="https://seclists.org">seclists.org</a>
[SECURITY] [DLA 1761-1] ghostscript security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>
[SECURITY] Fedora 28 Update: ghostscript-9.26-4.fc28 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 29 Update: ghostscript-9.26-4.fc29 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>
[SECURITY] Fedora 28 Update: ghostscript-9.26-4.fc28 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Slackware Security Advisory - ghostscript Updates ≈ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>
Ghostscript CVE-2019-3835 Security Bypass Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>
1677588 – (CVE-2019-3835) CVE-2019-3835 ghostscript: superexec operator is available (700585)	CONFIRM	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>
GPL Ghostscript: Multiple vulnerabilities (GLSA 202004-03) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>
[security-announce] openSUSE-SU-2019:2222-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
[SECURITY] Fedora 29 Update: ghostscript-9.26-4.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[security-announce] openSUSE-SU-2019:2223-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
[SECURITY] Fedora 30 Update: ghostscript-9.26-4.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 30 Update: ghostscript-9.26-4.fc30 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Debian -- Security Information -- DSA-4432-1 ghostscript	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>
Bugtraq: [slackware-security] ghostscript (SSA:2019-092-01)	BUGTRAQ	<a href="https://seclists.org">seclists.org</a>
700585 – is superexec still available ?	MISC	<a href="https://bugs.ghostscript.com">bugs.ghostscript.com</a>
CVE-2019-3835	CVE-2019-3835	

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[296080](#) Oracle Solaris 11.4 Support Repository Update (SRU) 13.4.0 Missing (CPUJUL2019)

[376886](#) Alibaba Cloud Linux Security Update for ghostscript (ALINUX2-SA-2019:0017)

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

[378226](#) Virtuozzo Linux Security Update for ghostscript-gtk (VZLSA-2019:0633)

[500210](#) Alpine Linux Security Update for ghostscript

[501408](#) Alpine Linux Security Update for ghostscript

[503953](#) Alpine Linux Security Update for ghostscript

© [CVE.report](http://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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://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](http://status.cve.report)**