



# CVE-2019-3838

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

## Summary

<b>CVE</b>	CVE-2019-3838
<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 forceput operator could be extracted from the DefineResource method in ghostscript before 9.27. A sp

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## 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>	42.3	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>	42.3	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Ansible Tower</a>	3.3	All	All	All

Application	Redhat	Ansible Tower	3.3	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	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	7.6	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	Source	Link
Bugtraq: [SECURITY] [DSA 4432-1] ghostscript security update	BUGTRAQ	<a href="#">seclists.org</a>
[SECURITY] [DLA 1761-1] ghostscript security update	MLIST	<a href="#">lists.debian.</a>
Red Hat Customer Portal	REDHAT	<a href="#">access.redh</a>
[SECURITY] Fedora 28 Update: ghostscript-9.26-4.fc28 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedorap</a>
[SECURITY] Fedora 29 Update: ghostscript-9.26-4.fc29 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedorap</a>
Red Hat Customer Portal	REDHAT	<a href="#">access.redh</a>
[SECURITY] Fedora 28 Update: ghostscript-9.26-4.fc28 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedorap</a>
700576 – forceput in DefineResource still accessible after CVE-2019-6116	MISC	<a href="#">bugs.ghosts</a>
[security-announce] openSUSE-SU-2019:1121-1: important: Security update	SUSE	<a href="#">lists.opensu</a>
Slackware Security Advisory - ghostscript Updates ≈ Packet Storm	MISC	<a href="#">packetstorm</a>
GPL Ghostscript: Multiple vulnerabilities (GLSA 202004-03) — Gentoo security	GENTOO	<a href="#">security.gen</a>
[SECURITY] Fedora 29 Update: ghostscript-9.26-4.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedorap</a>
[SECURITY] Fedora 30 Update: ghostscript-9.26-4.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedorap</a>
[SECURITY] Fedora 30 Update: ghostscript-9.26-4.fc30 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedorap</a>
Debian -- Security Information -- DSA-4432-1 ghostscript	DEBIAN	<a href="#">www.debian</a>
Security Advisory: CVE-2019-6116: Multiple vulnerabilities in Ghostscript	SUSE	<a href="#">suse.com</a>

[security-announce] opensUSE-SU-2019:1119-1: important: Security update	SUSE	<a href="https://lists.opensuse.org/">lists.opensuse.org</a>
1677581 – (CVE-2019-3838) CVE-2019-3838 ghostscript: forceput in DefineResource is still accessible (700576)	CONFIRM	<a href="https://bugzilla.redhat.com/">bugzilla.redhat.com</a>
Bugtraq: [slackware-security] ghostscript (SSA:2019-092-01)	BUGTRAQ	<a href="https://seclists.org/">seclists.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org/">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov/">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">296080</a> Oracle Solaris 11.4 Support Repository Update (SRU) 13.4.0 Missing (CPUJUL2019)
<a href="#">376886</a> Alibaba Cloud Linux Security Update for ghostscript (ALINUX2-SA-2019:0017)
<a href="#">377128</a> Alibaba Cloud Linux Security Update for ghostscript (ALINUX3-SA-2022:0123)
<a href="#">378226</a> Virtuozzo Linux Security Update for ghostscript-gtk (VZLSA-2019:0633)
<a href="#">500210</a> Alpine Linux Security Update for ghostscript
<a href="#">501408</a> Alpine Linux Security Update for ghostscript
<a href="#">503953</a> Alpine Linux Security Update for ghostscript

© [CVE.report](https://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](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve/). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)