



CVE-2019-6116

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2019-6116 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2019-03-21 16:01:00 UTC |
| Updated | 2023-11-07 03:13:00 UTC |
| Description | In Artifex Ghostscript through 9.26, ephemeral or transient procedures can allow access to system operators, leading to ren |

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-------------------------------|------------------------------|---------|--------|---------|----------|
| Application | Artifex | Ghostscript | All | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 14.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 14.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.10 | 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 | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Fedoraproject | Fedora | 28 | All | All | All |
| Operating System | Fedoraproject | Fedora | 29 | All | All | All |
| Operating System | Fedoraproject | Fedora | 30 | All | All | All |
| Operating System | Fedoraproject | Fedora | 28 | All | All | All |

| | | | | | | |
|------------------|-------------------------------|--|------|-----|-----|-----|
| Operating System | Fedoraproject | Fedora | 29 | All | All | All |
| Operating System | Fedoraproject | Fedora | 30 | All | All | All |
| Operating System | Opensuse | Leap | 15.0 | All | All | All |
| Operating System | Opensuse | Leap | 42.3 | All | All | All |
| Operating System | Opensuse | Leap | 15.0 | All | All | All |
| Operating System | Opensuse | Leap | 42.3 | 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 |
|--|------------|--|
| [SECURITY] Fedora 29 Update: ghostscript-9.26-3.fc29 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject.org |
| [SECURITY] Fedora 29 Update: ghostscript-9.27-1.fc29 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject.org |
| [SECURITY] Fedora 30 Update: ghostscript-9.26-3.fc30 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject.org |
| [SECURITY] Fedora 29 Update: ghostscript-9.27-1.fc29 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org |
| oss-security - ghostscript: 2 -dSAFER bypass: CVE-2019-3835 & CVE-2019-3838 | MLIST | www.openwall.com |
| Ghostscript 9.26 - Pseudo-Operator Remote Code Execution - Linux remote Exploit | EXPLOIT-DB | www.exploit-db.com |
| Slackware Security Advisory - ghostscript Updates ≈ Packet Storm | MISC | packetstormsecurity.com |
| 700317 – ghostscript: subroutines within pseudo-operators must themselves be pseudo-operators | CONFIRM | bugs.ghostscript.com |
| [SECURITY] Fedora 30 Update: ghostscript-9.27-1.fc30 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org |
| Ghostscript CVE-2019-6116 Remote Code Execution Vulnerability | BID | www.securityfocus.com |
| Debian -- Security Information -- DSA-4372-1 ghostscript | DEBIAN | www.debian.org |
| Red Hat Customer Portal | REDHAT | access.redhat.com |
| [SECURITY] Fedora 30 Update: ghostscript-9.27-1.fc30 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject.org |
| [SECURITY] [DLA 1670-1] ghostscript security update | MLIST | lists.debian.org |

| | | |
|---|---------|---|
| GPL Ghostscript: Multiple vulnerabilities (GLSA 202004-03) — Gentoo security | GENTOO | security.gentoo.org |
| USN-3866-1: Ghostscript vulnerability Ubuntu security notices Ubuntu | UBUNTU | usn.ubuntu.com |
| Ghostscript Pseudo-Operator Remote Code Execution ≈ Packet Storm | MISC | packetstormsecurity.com |
| [security-announce] openSUSE-SU-2019:0103-1: important: Security update | CONFIRM | lists.opensuse.org |
| [SECURITY] Fedora 28 Update: ghostscript-9.26-3.fc28 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org |
| oss-security - ghostscript: subroutines within pseudo-operators must themselves be pseudo-operators | MLIST | www.openwall.com |
| [security-announce] openSUSE-SU-2019:0104-1: important: Security update | CONFIRM | lists.opensuse.org |
| Issue 1729 - project-zero - Project Zero - Monorail | MISC | bugs.chromium.org |
| Red Hat Customer Portal | REDHAT | access.redhat.com |
| [SECURITY] Fedora 30 Update: ghostscript-9.26-3.fc30 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org |
| Bugtraq: [slackware-security] ghostscript (SSA:2019-092-01) | BUGTRAQ | seclists.org |
| [SECURITY] Fedora 29 Update: ghostscript-9.26-3.fc29 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org |
| [SECURITY] Fedora 28 Update: ghostscript-9.26-3.fc28 - 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

- [296080](#) Oracle Solaris 11.4 Support Repository Update (SRU) 13.4.0 Missing (CPUJUL2019)
- [296088](#) Oracle Solaris 11.4 Support Repository Update (SRU) 9.1.5 Missing (CPUAPR2019)
- [377128](#) Alibaba Cloud Linux Security Update for ghostscript (ALINUX3-SA-2022:0123)
- [377191](#) Alibaba Cloud Linux Security Update for ghostscript (ALINUX2-SA-2019:0003)
- [500210](#) Alpine Linux Security Update for ghostscript
- [501407](#) Alpine Linux Security Update for ghostscript
- [503952](#) 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://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org). This site includes MITRE data granted under the following [license](https://mitre.org).

CVE.report and Source URL Uptime Status status.cve.report