



CVE-2019-10216

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2019-10216 |
| State | PUBLIC |
| Assigner | secalert@redhat.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2019-11-27 13:15:00 UTC |
| Updated | 2023-11-07 03:02:00 UTC |
| Description | In ghostscript before version 9.50, the .buildfont1 procedure did not properly secure its privileged calls, enabling scripts to b |

Risk And Classification

Problem Types: NVD-CWE-Other

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 |
| Application | Redhat | 3scale Api Management | 2.6 | All | All | All |
| Application | Redhat | 3scale Api Management | 2.6 | 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 | 8.0 | 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 | 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 |

References

| Reference | Source | Link |
|--|---------|---|
| git.ghostscript.com Git - ghostpd.git/commitdiff | CONFIRM | git.ghostscript.com |
| 1737080 – (CVE-2019-10216) CVE-2019-10216 ghostscript: -dSAFER escape via .buildfont1 (701394) | CONFIRM | bugzilla.redhat.com |
| GPL Ghostscript: Multiple vulnerabilities (GLSA 202004-03) — Gentoo security | GENTOO | security.gentoo.org |
| git.ghostscript.com Git - ghostpd.git/commitdiff | | git.ghostscript.com |
| 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

[296079](#) Oracle Solaris 11.4 Support Repository Update (SRU) 15.5.0 Missing (CPUOCT2019)

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

[500211](#) Alpine Linux Security Update for ghostscript

[503954](#) 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