



# CVE-2020-16302

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2020-16302  |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | cve@mitre.org   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2020-08-13 03:15:00 UTC   |
| <b>Updated</b>         | 2023-11-07 03:18:00 UTC   |
| <b>Description</b>     | A buffer overflow vulnerability in jetp3852_print_page() in devices/gdev3852.c of Artifex Software GhostScript v9.50 allows |

## Risk And Classification

**Problem Types:** CWE-120

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                    | Product                      | Version | Update | Edition | Language |
|------------------|---------------------------|------------------------------|---------|--------|---------|----------|
| Application      | <a href="#">Artifex</a>   | <a href="#">Ghostscript</a>  | 9.50    | All    | All     | All      |
| Application      | <a href="#">Artifex</a>   | <a href="#">Ghostscript</a>  | 9.50    | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 16.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 18.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 20.04   | All    | All     | All      |
| Operating System | <a href="#">Debian</a>    | <a href="#">Debian Linux</a> | 10.0    | 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> | 9.0     | All    | All     | All      |

## References

| Reference  | Source | Link                                 | Tags                |
|--|--------|--------------------------------------|---------------------|
| git.ghostscript.com Git - ghostpdl.git/commitdiff                                |        | <a href="#">git.ghostscript.com</a>  |                     |
| git.ghostscript.com Git - ghostpdl.git/commitdiff                                | MISC   | <a href="#">git.ghostscript.com</a>  | Patch, Vendor Adv   |
| 701815 – global-buffer-overflow at devices/gdev3852.c:122 in jetp3852_print_page | MISC   | <a href="#">bugs.ghostscript.com</a> | Exploit, Issue Trac |
| [SECURITY] [DLA 2335-1] ghostscript security update                              | MLIST  | <a href="#">lists.debian.org</a>     | Third Party Adviso  |
| GPL Ghostscript: Multiple vulnerabilities (GLSA 202008-20) — Gentoo security     | GENTOO | <a href="#">security.gentoo.org</a>  | Third Party Adviso  |
| Debian -- Security Information -- DSA-4748-1 ghostscript                         | DEBIAN | <a href="#">www.debian.org</a>       | Third Party Adviso  |

|  |         |   |                     |
|--|---------|---|---------------------|
| USN-4469-1: Ghostscript vulnerabilities   Ubuntu security notices   Ubuntu | UBUNTU  | <a href="https://usn.ubuntu.com">usn.ubuntu.com</a> |                     |
| CVE Program record   | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>       | canonical           |
| NVD vulnerability detail   | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>     | canonical, analysis |

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[159222](#) Oracle Enterprise Linux Security Update for ghostscript (ELSA-2021-1852)

[239294](#) Red Hat Update for ghostscript (RHSA-2021:1852)

[501409](#) Alpine Linux Security Update for ghostscript

[503958](#) Alpine Linux Security Update for ghostscript

[940105](#) AlmaLinux Security Update for ghostscript (ALSA-2021:1852)

[960364](#) Rocky Linux Security Update for ghostscript (RLSA-2021:1852)

© [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](#)