



# CVE-2020-27792

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

## Summary

<b>CVE</b>	CVE-2020-27792
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-08-19 23:15:00 UTC
<b>Updated</b>	2023-12-19 06:15:00 UTC
<b>Description</b>	A heap-based buffer over write vulnerability was found in GhostScript's lp8000_print_page() function in gdevlp8k.c file. An a

## Risk And Classification

**Problem Types:** CWE-119

## 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
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All

## References

### Reference

- 701844 – heap-buffer-overflow at devices/gdevlp8k.c:330 in lp8000\_print\_page
- [SECURITY] [DLA 3096-1] ghostscript security update
- [git.ghostscript.com Git - ghostpd.git/commitdiff](#)
- [git.ghostscript.com Git - ghostpd.git/commitdiff](#)
- 2247179 – (CVE-2020-27792) CVE-2020-27792 ghostscript: heap buffer over write vulnerability in GhostScript's lp8000\_print\_page() in gdevlp8k.c
- [cve-details](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

180991 Debian Security Update for ghostscript (DLA 3096-1)
198965 Ubuntu Security Notification for Ghostscript Vulnerabilities (USN-5643-1)
354776 Amazon Linux Security Advisory for ghostscript : ALAS2-2023-1947
354856 Amazon Linux Security Advisory for ghostscript : ALAS-2023-1725
355071 Amazon Linux Security Advisory for ghostscript : AL2012-2023-395
673099 EulerOS Security Update for ghostscript (EulerOS-SA-2023-2144)

© [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](#)