



CVE-2023-40032

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

Summary

CVE	CVE-2023-40032
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-11 19:15:00 UTC
Updated	2024-01-29 07:15:00 UTC
Description	libvips is a demand-driven, horizontally threaded image processing library. A specially crafted SVG input can cause libvips v

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libvips	Libvips	All	All	All	All

References

Reference	Source
svgload: fix null-pointer dereference (#3604) · libvips/libvips@e091d65 · GitHub	MISC
Potential segfault due to NULL pointer dereference when parsing specially crafted SVG input · Advisory · libvips/libvips · GitHub	MISC
svgload: fix null-pointer dereference by kleisauke · Pull Request #3604 · libvips/libvips · GitHub	MISC
[SECURITY] Fedora 39 Update: vips-8.15.1-1.fc39 - package-announce - Fedora Mailing-Lists	
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[199837](#) Ubuntu Security Notification for VIPS Vulnerabilities (USN-6437-1)

[285024](#) Fedora Security Update for vips (FEDORA-2024-5c3c77b8eb)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)