CVE-2017-9739

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-9739
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-26 19:29:00 UTC
Updated	2023-11-07 02:50:00 UTC
Description	The Ins_JMPR function in base/ttinterp.c in Artifex Ghostscript GhostXPS 9.21 allows remote attackers to cause a denial of

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Artifex	Ghostscript Ghostxps	9.21	All	All	All
Application	Artifex	Ghostscript Ghostxps	9.21	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

References

Reference	Source	Link	Tags
Ghostscript GhostXPS CVE-2017-9739 Heap Buffer Overflow Vulnerability	BID	www.securityfocus.com	Third Party Advisory,
git.ghostscript.com Git - ghostpdl.git/commit		git.ghostscript.com	
Debian -- Security Information -- DSA-3986-1 ghostscript	DEBIAN	www.debian.org	Third Party Advisory
git.ghostscript.com Git - ghostpdl.git/commit	CONFIRM	git.ghostscript.com	Third Party Advisory
GPL Ghostscript: Multiple vulnerabilities (GLSA 201811-12) — Gentoo security	GENTOO	security.gentoo.org	Third Party Advisory
Bug 698063 – heap-buffer-overflow in Ins_JMPR(base/ttinterp.c)	CONFIRM	bugs.ghostscript.com	Exploit, Issue Trackir
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

670288 EulerOS Security Update for ghostscript (EulerOS-SA-2021-1788)

670614 EulerOS Security Update for ghostscript (EulerOS-SA-2021-2372)

710304 Gentoo Linux GPL Ghostscript Multiple Vulnerabilities (GLSA 201811-12)

© 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 registred 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