CVE-2018-17961

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-17961
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-15 16:29:00 UTC
Updated	2023-11-07 02:54:00 UTC
Description	Artifex Ghostscript 9.25 and earlier allows attackers to bypass a sandbox protection mechanism via vectors involving errorh

Risk And Classification

Problem Types: CWE-209

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
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	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
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	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	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
ghostscript - executeonly Bypass with errorhandler Setup - Linux local Exploit	EXPLOIT-DB	www.exploit-db.com
699816 – executeonly bypass with errorhandler setup	CONFIRM	bugs.ghostscript.com
USN-3803-1: Ghostscript vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
Debian -- Security Information -- DSA-4336-1 ghostscript	DEBIAN	www.debian.org
git.ghostscript.com Git - ghostpdl.git/commitdiff		git.ghostscript.com
git.ghostscript.com Git - ghostpdl.git/commitdiff	CONFIRM	git.ghostscript.com
git.ghostscript.com Git - ghostpdl.git/commitdiff	CONFIRM	git.ghostscript.com
git.ghostscript.com Git - ghostpdl.git/commitdiff	CONFIRM	git.ghostscript.com
Red Hat Customer Portal	REDHAT	access.redhat.com
oss-security - ghostscript: bypassing executeonly to escape -dSAFER sandbox (CVE-2018-17961)	MLIST	www.openwall.com
1682 - ghostscript: executeonly bypass with errorhandler setup - project-zero - Monorail	MISC	bugs.chromium.org
git.ghostscript.com Git - ghostpdl.git/commitdiff		git.ghostscript.com
git.ghostscript.com Git - ghostpdl.git/commitdiff		git.ghostscript.com
[SECURITY] [DLA 1552-1] ghostscript security update	MLIST	lists.debian.org
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

500208 Alpine Linux Security Update for ghostscript

503950 Alpine Linux Security Update for ghostscript