CVE-2016-3622

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-3622
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-10-03 16:09:00 UTC
Updated	2017-11-04 01:29:00 UTC
Description	The fpAcc function in tif_predict.c in the tiff2rgba tool in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial

Risk And Classification

Problem Types: CWE-369

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libtiff	Libtiff	4.0.6	All	All	All
Application	Libtiff	Libtiff	4.0.6	All	All	All

References

Reference	Source
Debian -- Security Information -- DSA-3762-1 tiff	DEBIAN
libTIFF: Multiple vulnerabilities (GLSA 201701-16) — Gentoo Security	GENTOO
LibTIFF CVE-2016-3622 Divide By Zero Denial of Service Vulnerability	BID
LibTIFF Divide-by-Zero Error and Multiple Read Errors Let Remote Users Cause the Target Application to Crash - SecurityTracker	SECTRA
oss-security - CVE-2016-3622 libtiff: Divide By Zero in the tiff2rgba tool	MLIST
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710479 Gentoo Linux libTIFF Multiple Vulnerabilities (GLSA 201701-16)

© 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