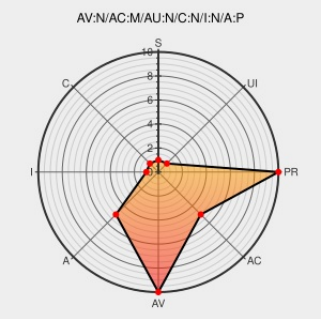
CVE-2010-2597

Published on: 07/01/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:10 PM UTC

CVE-2010-2597

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Libtiff from Libtiff contain the following vulnerability:

The TIFFVStripSize function in tif_strip.c in LibTIFF 3.9.0 and 3.9.2 makes incorrect calls to the TIFFGetField function, which allows remote attackers to cause a denial of service (application crash) via a crafted TIFF image, related to "downsampled OJPEG input" and possibly related to a compiler optimization that triggers a divide-by-zero error.

CVE-2010-2597 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Bug 2215 – Incorrect uses of TIFFGetField where TIFFGetFieldDefaulted is needed	bugzilla.maptools.org text/html	CONFIRM bugzilla.maptools.org/show_bug.cgi?id=2215
LibTIFF Denial of Service Vulnerabilities - Advisories - Community	web.archive.org text/html	SECUNIA 40422
Debian -- Security Information -- DSA-2552-1 tiff	www.debian.org Depreciated Link text/html	DEBIAN DSA-2552
Support	www.redhat.com text/html	REDHAT RHSA-2010:0519
Security Advisory SA50726 - Gentoo update for tiff - Secunia	web.archive.org text/html	SECUNIA 50726

Bug 583081 – Assorted libtiff failures on downsampled OJPEG input	Exploit bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=583081
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2010-1761
Red Hat update for libtiff - Advisories - Community	web.archive.org text/html	SECUNIA 40527
Bug #593067 “eog crashed with SIGSEGV in __memset_sse2()” : Bugs : tiff package : Ubuntu	bugs.launchpad.net text/html	CONFIRM bugs.launchpad.net/bugs/593067
Gentoo Linux Documentation -- libTIFF: Multiple vulnerabilities	security.gentoo.org text/html	GENTOO GLSA-201209-02
Bug 603703 – libtiff: TIFFReadEncodedStrip crash	Patch bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=603703

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libtiff	Libtiff	3.9.0	All	All	All
Application	Libtiff	Libtiff	3.9.2	All	All	All
Application	Libtiff	Libtiff	3.9.0	All	All	All
Application	Libtiff	Libtiff	3.9.2	All	All	All

cpe:2.3:a:libtiff:libtiff:3.9.0:*:*:*:*:*:*:*:

cpe:2.3:a:libtiff:libtiff:3.9.2:*:*:*:*:*:*:*:

cpe:2.3:a:libtiff:libtiff:3.9.0:*:*:*:*:*:*:*:

cpe:2.3:a:libtiff:libtiff:3.9.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 |
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