

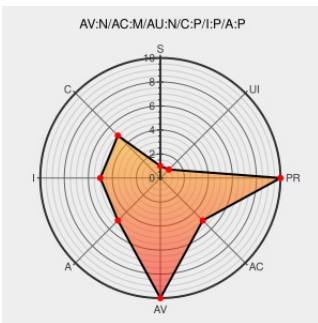


CVE-2013-4232

Published on: 09/10/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:45:00 AM UTC

CVE-2013-4232

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

Use-after-free vulnerability in the `t2p_readwrite_pdf_image` function in `tools/tiff2pdf.c` in `libtiff 4.0.3` allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted TIFF image.

CVE-2013-4232 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

LibTiff Mailing List Archive, "Vulnerabilities in libtiff 4.0.3", by Pedro Ribeiro

www.asmail.be
text/html

[MLIST \[tiff\] 20130801 Vulnerabilities in libtiff 4.0.3](#)

Debian -- Security Information -- DSA-2744-1 tiff

www.debian.org
Deprecated Link
text/html

[DEBIAN DSA-2744](#)

995975 -- (CVE-2013-4232) CVE-2013-4232 libtiff (tiff2pdf): use-after-free in `t2p_readwrite_pdf_image()`

Patch
bugzilla.redhat.com
text/html

[CONFIRM bugzilla.redhat.com/show_bug.cgi?id=995975](https://bugzilla.redhat.com/show_bug.cgi?id=995975)

Red Hat Customer Portal

web.archive.org
text/html
Inactive Link **Not Archived**

[REDHAT RHSA-2014:0223](#)

access.redhat.com | CVE-2013-4232

access.redhat.com
text/html

[MISC access.redhat.com/security/cve/CVE-2013-4232](https://access.redhat.com/security/cve/CVE-2013-4232)

Security Advisory SA54543 - Debian update for tiff - Secunia	Vendor Advisory web.archive.org text/html	 SECUNIA 54543
oss-security - Re: CVE Request -- Four (stack-based) buffer overflows and one use-after-free in libtiff v4.0.3 reported by Pedro Ribeiro	www.openwall.com text/html	 MLIST [oss-security] 20130809 Re: CVE Request -- Four (stack-based) buffer overflows and one use-after-free in libtiff v4.0.3 reported by Pedro Ribeiro
About Secunia Research Flexera	Vendor Advisory secunia.com Deprecated Link text/plain	 SECUNIA 54628
Red Hat Customer Portal	access.redhat.com text/html	 MISC access.redhat.com/errata/RHSA-2014:0223
Red Hat Customer Portal	access.redhat.com text/html	 MISC access.redhat.com/errata/RHSA-2014:0222
Bug 2449 – tiff2pdf: Use-after-free in t2p_readwrite_pdf_image()	Patch bugzilla.maptools.org text/html	 CONFIRM bugzilla.maptools.org/show_bug.cgi?id=2449

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
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	Libtiff	Libtiff	4.0.3	All	All	All
Application	Libtiff	Libtiff	4.0.3	All	All	All
cpe:2.3:o:debian:debian_linux:6.0:*****:.*						
cpe:2.3:o:debian:debian_linux:7.0:*****:.*						
cpe:2.3:o:debian:debian_linux:6.0:*****:.*						
cpe:2.3:o:debian:debian_linux:7.0:*****:.*						
cpe:2.3:a:libtiff:libtiff:4.0.3:*****:.*						

cpe:2.3:a:libtiff:libtiff:4.0.3:*****::

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 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](#).

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