



CVE-2004-1308

Published on: 12/22/2004 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:10 PM UTC

CVE-2004-1308

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

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

Integer overflow in (1) `tif_dirread.c` and (2) `tif_fax3.c` for libtiff 3.5.7 and 3.7.0 allows remote attackers to execute arbitrary code via a TIFF file containing a TIFF_ASCII or TIFF_UNDEFINED directory entry with a -1 entry count, which leads to a heap-based buffer overflow.

CVE-2004-1308 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Home - Conectiva

[distro.conectiva.com.br](#)
[text/html](#)

[CONECTIVA CLA-2005:920](#)

[rhn.redhat.com](#) | Red Hat Support

[www.redhat.com](#)
[text/html](#)

[REDHAT RHSA-2005:019](#)

Repository / Oval Repository

[oval.cisecurity.org](#)
[text/html](#)

[OVAL](#)
[oval:org.mitre.oval:def:100117](#)

404 Page Not Found | SUSE

[web.archive.org](#)
[text/html](#)
Inactive Link **Not Archived**

[SUSE SUSE-SA:2005:001](#)

US-CERT Vulnerability Note VU#125598

[US Government Resource](#)
[www.kb.cert.org](#)
[text/html](#)

[CERT-VN VU#125598](#)

IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF libtiff-tiff-tdircount-bo(18637)
iDEFENSE	Exploit Patch Vendor Advisory www.idefense.com text/html	 IDEFENSE 20041221 libtiff Directory Entry Count Integer Overflow Vulnerability
US-CERT Technical Cyber Security Alert TA05-136A -- Apple Mac OS X is affected by multiple vulnerabilities	US Government Resource www.us-cert.gov text/html	 CERT TA05-136A
Resend: APPLE-SA-2005-05-03 Security Update 2005-005	lists.apple.com text/html	 APPLE APPLE-SA-2005-05-03
Advisories - Mandriva	www.mandriva.com text/html	 MANDRAKE MDKSA-2005:052
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2005:035
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval.org.mitre.oval:def:9392
#101677: Multiple Security Vulnerabilities in libtiff(3) (formerly Document ID: 57769)	web.archive.org text/html Inactive Link Not Archived	 SUNALERT 101677
Debian -- Security Information -- DSA-617-1 tiff	www.debian.org Deprecated Link text/html	 DEBIAN DSA-617
No Description Provided	sunsolve.sun.com Inactive Link Not Archived	 SUNALERT 201072
Secunia - Advisories - SUSE update for libtiff/tiff	web.archive.org text/html	 SECUNIA 13776

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	3.4	All	All	All
Application	Libtiff	Libtiff	3.5.1	All	All	All
Application	Libtiff	Libtiff	3.5.2	All	All	All
Application	Libtiff	Libtiff	3.5.3	All	All	All
Application	Libtiff	Libtiff	3.5.4	All	All	All
Application	Libtiff	Libtiff	3.5.5	All	All	All
Application	Libtiff	Libtiff	3.5.7	All	All	All

Application	Libtiff	Libtiff	3.6.0	All	All	All
Application	Libtiff	Libtiff	3.6.1	All	All	All
Application	Libtiff	Libtiff	3.7.0	All	All	All
Application	Libtiff	Libtiff	3.4	All	All	All
Application	Libtiff	Libtiff	3.5.1	All	All	All
Application	Libtiff	Libtiff	3.5.2	All	All	All
Application	Libtiff	Libtiff	3.5.3	All	All	All
Application	Libtiff	Libtiff	3.5.4	All	All	All
Application	Libtiff	Libtiff	3.5.5	All	All	All
Application	Libtiff	Libtiff	3.5.7	All	All	All
Application	Libtiff	Libtiff	3.6.0	All	All	All
Application	Libtiff	Libtiff	3.6.1	All	All	All
Application	Libtiff	Libtiff	3.7.0	All	All	All
cpe:2.3:a:libtiff:libtiff:3.4:*:*:*:*:*:						
cpe:2.3:a:libtiff:libtiff:3.5.1:*:*:*:*:*:						
cpe:2.3:a:libtiff:libtiff:3.5.2:*:*:*:*:*:						
cpe:2.3:a:libtiff:libtiff:3.5.3:*:*:*:*:*:						
cpe:2.3:a:libtiff:libtiff:3.5.4:*:*:*:*:*:						
cpe:2.3:a:libtiff:libtiff:3.5.5:*:*:*:*:*:						
cpe:2.3:a:libtiff:libtiff:3.5.7:*:*:*:*:*:						
cpe:2.3:a:libtiff:libtiff:3.6.0:*:*:*:*:*:						
cpe:2.3:a:libtiff:libtiff:3.6.1:*:*:*:*:*:						
cpe:2.3:a:libtiff:libtiff:3.7.0:*:*:*:*:*:						
cpe:2.3:a:libtiff:libtiff:3.4:*:*:*:*:*:						
cpe:2.3:a:libtiff:libtiff:3.5.1:*:*:*:*:*:						
cpe:2.3:a:libtiff:libtiff:3.5.2:*:*:*:*:*:						
cpe:2.3:a:libtiff:libtiff:3.5.3:*:*:*:*:*:						
cpe:2.3:a:libtiff:libtiff:3.5.4:*:*:*:*:*:						
cpe:2.3:a:libtiff:libtiff:3.5.5:*:*:*:*:*:						
cpe:2.3:a:libtiff:libtiff:3.5.7:*:*:*:*:*:						
cpe:2.3:a:libtiff:libtiff:3.6.0:*:*:*:*:*:						

cpe:2.3:a:libtiff:libtiff:3.6.1:*:*:*:*:*:

cpe:2.3:a:libtiff:libtiff:3.7.0:*:*:*:*:*:

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](#)