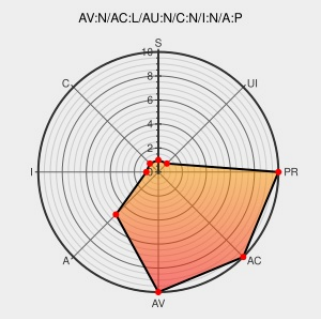
CVE-2005-2452

Published on: 08/03/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:28 PM UTC

CVE-2005-2452

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



Certain versions of Libtiff from Libtiff contain the following vulnerability:

libtiff up to 3.7.0 allows remote attackers to cause a denial of service (application crash) via a TIFF image header with a zero "YCbCr subsampling" value, which causes a divide-by-zero error in (1) tif_strip.c and (2) tif_tile.c, a different vulnerability than CVE-2004-0804.

CVE-2005-2452 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Advisories - Mandriva	www.mandriva.com text/html	MANDRAKE MDKSA-2005:143
Advisories - Mandriva	www.mandriva.com text/html	MANDRAKE MDKSA-2005:142
USN-156-1: TIFF vulnerability | Ubuntu security notices	usn.ubuntu.com text/html	UBUNTU USN-156-1
No Description Provided	bugzilla.ubuntu.com Inactive Link Not Archived	MISC bugzilla.ubuntu.com/show_bug.cgi?id=12008
Secunia - Advisories - Ubuntu update for libtiff4	Vendor Advisory web.archive.org text/html	SECUNIA 16266

Advisories - Mandriva	www.mandriva.com text/html	MANDRAKE MDKSA-2005:144
Secunia - Advisories - Mandriva update for libtiff	Vendor Advisory web.archive.org text/html	SECUNIA 16486
LibTiff Tiff Image Header Divide By Zero Denial of Service Vulnerability	cve.report (archive) text/html	BID 14417

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	3.5.5	All	All	All
Application	Libtiff	Libtiff	3.5.7	All	All	All
Application	Libtiff	Libtiff	3.6.1	All	All	All
Application	Libtiff	Libtiff	3.5.5	All	All	All
Application	Libtiff	Libtiff	3.5.7	All	All	All
Application	Libtiff	Libtiff	3.6.1	All	All	All

cpe:2.3:a:libtiff:libtiff:3.5.5:*:*:*:*:*:*:*:

cpe:2.3:a:libtiff:libtiff:3.5.7:*:*:*:*:*:*:*:

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

cpe:2.3:a:libtiff:libtiff:3.5.5:*:*:*:*:*:*:*:

cpe:2.3:a:libtiff:libtiff:3.5.7:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report