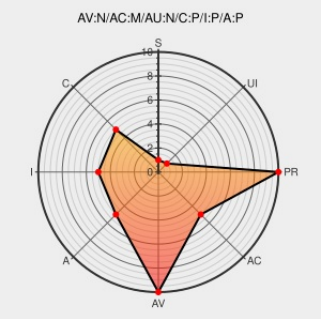
CVE-2010-2067

Published on: 06/23/2010 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:19:00 AM UTC

CVE-2010-2067

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



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

Stack-based buffer overflow in the TIFFFetchSubjectDistance function in tif_dirread.c in LibTIFF before 3.9.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long EXIF SubjectDistance field in a TIFF file.

CVE-2010-2067 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
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:014	Mailing List, Third Party Advisory, lists.opensuse.org, text/html	SUSE SUSE-SR:2010:014
Public Advisory: 06.21.10 // iDefense Labs	Broken Link, web.archive.org, text/html, Inactive Link, Not Archived	IDEFENSE 20100621 Multiple Vendor LibTIFF 3.9.2 Stack Buffer Overflow Vulnerability
Bug 599576 – CVE-2010-2067 libtiff: SubjectDistance EXIF tag reading stack based buffer overflow	Issue Tracking, Third Party Advisory, bugzilla.redhat.com, text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=599576
Bug 2212 – Inadequate validation of SubjectDistance tag	Issue Tracking, Third Party Advisory	CONFIRM bugzilla.maptools.org/show_bug.cgi?id=2212

	bugzilla.maptools.org text/html	
Security Advisory SA50726 - Gentoo update for tiff - Secunia	Third Party Advisory web.archive.org text/html	SECUNIA 50726
Changes in TIFF v3.9.4	Broken Link web.archive.org text/html Inactive Link Not Archived	CONFIRM www.remotesensing.org/libtiff/v3.9.4.html
Slackware update for libtiff - Advisories - Community	Third Party Advisory web.archive.org text/html	SECUNIA 40381
'[oss-security] CVE requests: LibTIFF' - MARC	Mailing List Third Party Advisory marc.info text/html	MLIST [oss-security] 20100623 CVE requests: LibTIFF
USN-954-1: tiff vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-954-1
No Description Provided	Broken Link osvdb.org Inactive Link Not Archived	OSVDB 65676
Gentoo Linux Documentation -- libTIFF: Multiple vulnerabilities	Third Party Advisory security.gentoo.org text/html	GENTOO GLSA-201209-02
Webmail - OVH	Third Party Advisory www.vupen.com text/html	VUPEN ADV-2010-1638
CVE-2010-2067 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2010-2067
The Slackware Linux Project: Slackware Security Advisories	Third Party Advisory slackware.com text/html	SLACKWARE SSA:2010-180-02
About Secunia Research | Flexera	Third Party Advisory secunia.com Depreciated Link text/plain	SECUNIA 40241

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All

System						
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Application	Libtiff	Libtiff	All	All	All	All
Application	Libtiff	Libtiff	All	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:6.06:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:8.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:9.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:9.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:6.06:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:8.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:9.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:9.10:*:*:*:*:*:*:*:

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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