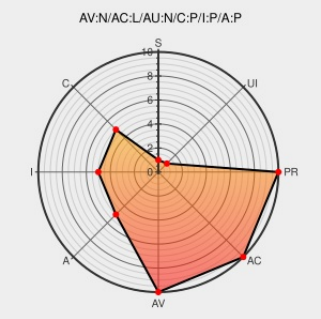
CVE-2006-2656

Published on: 05/30/2006 12:00:00 AM UTC

Last Modified on: 11/07/2023 01:58:00 AM UTC

CVE-2006-2656

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



Certain versions of Libtiff from Libtiff contain the following vulnerability:

Stack-based buffer overflow in the tiffsplit command in libtiff 3.8.2 and earlier might might allow attackers to execute arbitrary code via a long filename. NOTE: tiffsplit is not setuid. If there is not a common scenario under which tiffsplit is called with attacker-controlled command line arguments, then perhaps this issue should not be included in CVE.

CVE-2006-2656 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Ubuntu update for tiff - Advisories - Secunia	Vendor Advisory, web.archive.org, text/html	SECUNIA 20501
Debian update for tiff - Advisories - Secunia	Vendor Advisory, web.archive.org, text/html	SECUNIA 20520
Gentoo update for tiff - Advisories - Secunia	Vendor Advisory, web.archive.org, text/html	SECUNIA 21002
[SECURITY] Fedora Core 4 Update: libtiff-3.7.1-6.fc4.2	Patch, www.redhat.com, text/html	FEDORA FEDORA-2006-591
USN-289-1: tiff vulnerabilities | Ubuntu security notices	usn.ubuntu.com	UBUNTU USN-289-1

	text/html	
SUSE Updates for Multiple Packages - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 20766
Debian -- Security Information -- DSA-1091-1 tiff	www.debian.org Depreciated Link text/html	DEBIAN DSA-1091
SuSE Security announcements: [suse-security-announce] SUSE Security Summary Report SUSE-SR:2006:014	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SR:2006:014
Advisories - Mandriva Linux	www.mandriva.com text/html	MANDRIVA MDKSA-2006:095
Gentoo Linux Documentation -- libTIFF: Multiple buffer overflows	security.gentoo.org text/html	GENTOO GLSA-200607-03
No Description Provided	marc.info text/html	VULN-DEV 20060524 tiffsplit (libtiff <= 3.8.2) bss & stack buffer overflow...

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	3.5.6	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	3.7.1	All	All	All
Application	Libtiff	Libtiff	3.8.0	All	All	All
Application	Libtiff	Libtiff	3.8.1	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	3.5.6	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	3.7.1	All	All	All
Application	Libtiff	Libtiff	3.8.0	All	All	All
Application	Libtiff	Libtiff	3.8.1	All	All	All
Application	Libtiff	Libtiff	All	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:3.5.6:*:*:*:*:*:*:*:

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:3.7.1:*:*:*:*:*:*:*:

cpe:2.3:a:libtiff:libtiff:3.8.0:*:*:*:*:*:*:*:

cpe:2.3:a:libtiff:libtiff:3.8.1:*:*:*:*:*:*:*:

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:3.5.6:*:*:*:*:*:*:*:

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:3.7.1:*:*:*:*:*:*:*:

cpe:2.3:a:libtiff:libtiff:3.8.0:*:*:*:*:*:*:*:

cpe:2.3:a:libtiff:libtiff:3.8.1:*:*:*:*:*:*:*:

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

← Previous ID

Next ID→