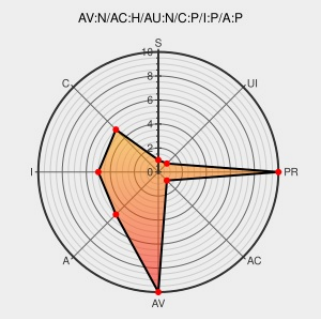
CVE-2004-1183

Published on: 01/06/2005 05:00:00 AM UTC

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

CVE-2004-1183

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



Certain versions of Libtiff from Libtiff contain the following vulnerability:

Integer overflow in the tiffdump utility for libtiff 3.7.1 and earlier allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a crafted TIFF file.

CVE-2004-1183 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5.1 - MEDIUM

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

CVE References

Description	Tags	Link
Home - Conectiva	distro.conectiva.com.br, text/html	CONECTIVA CLA-2005:920
LibTIFF TIFFDUMP Heap Corruption Integer Overflow Vulnerability	cve.report (archive), text/html	BID 12173
'[USN-54-1] TIFF library tool vulnerability' - MARC	marc.info, text/html	BUGTRAQ 20050106 [USN-54-1] TIFF library tool vulnerability
rhn.redhat.com | Red Hat Support	www.redhat.com, text/html	REDHAT RHSA-2005:019
404 Page Not Found | SUSE	Patch, web.archive.org, text/html, Inactive Link, Not Archived	SUSE SUSE-SA:2005:001

Advisories - Mandriva	www.mandriva.com text/html	MANDRAKE MDKSA-2005:001
Advisories - Mandriva	www.mandriva.com text/html	MANDRAKE MDKSA-2005:002
Secunia - Advisories - LibTIFF Unspecified tiffdump Integer Overflow Vulnerability	web.archive.org text/html	SECUNIA 13728
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF libtiff-tiffdump-bo(18782)
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:9743
Debian -- Page not found	www.debian.org Depreciated Link text/html Inactive Link Not Archived	DEBIAN DSA-626
Gentoo Linux Documentation -- tiff: New overflows in image decoding	Patch security.gentoo.org text/html	GENTOO GLSA-200501-06
Secunia - Advisories - SUSE update for libtiff/tiff	web.archive.org text/html	SECUNIA 13776

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	3.4	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

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:3.4:*:*:*:*:*:*:*:

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:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→