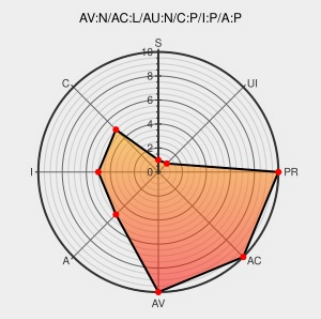
CVE-2005-3350

Published on: 11/03/2005 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:10:42 AM UTC

CVE-2005-3350

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



Certain versions of Libungif from Libungif contain the following vulnerability:

libungif library before 4.1.0 allows attackers to corrupt memory and possibly execute arbitrary code via a crafted GIF file that leads to an out-of-bounds write.

CVE-2005-3350 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
	scary.beasts.org text/plain	MISC scary.beasts.org/security/CESA-2005-007.txt
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:9314
Gentoo update for giflib - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	SECUNIA 17482
Gentoo Bug 109997 - media-libs/giflib: buffer overflow / null pointer deref	bugs.gentoo.org text/html	MISC bugs.gentoo.org/show_bug.cgi?id=109997
SecurityFocus	www.securityfocus.com text/html	FEDORA FLSA:174479
Secunia - Advisories - Ubuntu update for libungif	web.archive.org text/html	SECUNIA 17488

Debian -- Security Information -- DSA-890-1 libungif4	www.debian.org Depreciated Link text/html	DEBIAN DSA-890
Security Advisory SA34872 - Red Hat update for giflib - Secunia	web.archive.org text/html	SECUNIA 34872
SecurityTracker.com Archives - libungif NULL Pointer Dereference and Memory Access Error May Let Remote Users Execute Arbitrary Code	securitytracker.com text/html	SECTRACK 1015149
Libungif Colormap Handling Memory Corruption Vulnerability	cve.report (archive) text/html	BID 15299
Fedora update for giflib - Secunia Advisories - Vulnerability Information - Secunia.com	web.archive.org text/html	SECUNIA 35164
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 20471
Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	www.vupen.com inode/x-empty	VUPEN ADV-2005-2295
171413 – CVE-2005-2974 Several libungif issues (CVE-2005-3350)	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/bugzilla/show_bug.cgi?id=171413
Secunia - Advisories - SUSE Updates for Multiple Packages	web.archive.org text/html	SECUNIA 17559
Gentoo Linux Documentation -- giflib: Multiple vulnerabilities	www.gentoo.org text/html	GENTOO GLSA-200511-03
giflib GIF File Handling Two Vulnerabilities - Advisories - Secunia	web.archive.org text/html	SECUNIA 17462
SourceForge.net: giflib -- A library for processing GIFs: Files	web.archive.org text/html Inactive Link Not Archived	CONFIRM sourceforge.net/project/shownotes.php?release_id=364493
[SECURITY] Fedora 9 Update: giflib-4.1.3-10.fc9	www.redhat.com text/html	FEDORA FEDORA-2009-5118
Secunia - Advisories - Fedora update for libungif	web.archive.org text/html	SECUNIA 17438
Secunia - Advisories - Debian update for libungif4	web.archive.org text/html	SECUNIA 17497
SecurityFocus	www.securityfocus.com text/html	FEDORA FLSA-2006:174479
USN-214-1: libungif vulnerabilities | Ubuntu security notices | Ubuntu	www.ubuntulinux.org text/html	UBUNTU USN-214-1
Secunia - Advisories - Red Hat update for libungif	web.archive.org text/html	SECUNIA 17442
rhn.redhat.com | Red Hat Support	Vendor Advisory www.redhat.com text/html	REDHAT RHSA-2005:828
Secunia - Advisories - Mandriva update for libungif	web.archive.org text/html	SECUNIA 17508
Support	www.redhat.com	REDHAT RHSA-2009:0444

	text/html	
Secunia - Advisories - libungif GIF File Handling Two Vulnerabilities	web.archive.org text/html	SECUNIA 17436
Advisories - Mandriva Linux OS	www.mandriva.com text/html	MANDRIVA MDKSA-2005:207

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	Libungif	Libungif	4.1.3	All	All	All
Application	Libungif	Libungif	4.1.3	All	All	All
Application	Libungif	Libungif	All	All	All	All

cpe:2.3:a:libungif:libungif:4.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:libungif:libungif:4.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:libungif:libungif:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→