

CVE Details

The ultimate security vulnerability datasource

Log InRegisterReset PasswordActivate Account

Vulnerability Feeds & WidgetsNewwww.itsecdb.com

f

t

e

r

M

+

Home

Browse :

Vendors

Products

Vulnerabilities By Date

Vulnerabilities By Type

Reports :

CVSS Score Report

CVSS Score Distribution

Search :

Vendor Search

Product Search

Version Search

Vulnerability Search

By Microsoft References

Top 50 :

Vendors

Vendor Cvss Scores

Products

Product Cvss Scores

Versions

Other :

Microsoft Bulletins

Bugtraq Entries

CWE Definitions

About & Contact

Feedback

CVE Help

FAQ

Articles

External Links :

NVD Website

CWE Web Site

View CVE :

Go

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View BID :

Go

(e.g.: 12345)

Search By Microsoft Reference ID:

Go

(e.g.: ms10-001 or 979352)

Vulnerability Details : CVE-2006-2923

The iax_net_read function in the iaxclient open source library, as used in multiple products including (a) LoudHush 1.3.6, (b) IDE FISK 1.35 and earlier, (c) Kiax 0.8.5 and earlier, (d) DIAx, (e) Ziaxphone, (f) IAX Phone, (g) X-lite, (h) MediaX, (i) Extreme Networks ePhone, and (j) iaxComm before 1.2.0, allows remote attackers to execute arbitrary code via crafted IAX 2 (IAX2) packets with truncated (1) full frames or (2) mini-frames, which are detected in a length check but still processed, leading to buffer overflows related to negative length values.

Publish Date : 2006-06-09 Last Update Date : 2011-03-28

Collapse AllExpand AllSelectSelect&Copy

▼ Scroll To▼ Comments▼ External Links

Search Twitter

Search YouTube

Search Google

– CVSS Scores & Vulnerability Types

CVSS Score

6.4

Confidentiality Impact

Partial (There is considerable informational disclosure.)

Integrity Impact

Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)

Availability Impact

None (There is no impact to the availability of the system.)

Access Complexity

Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)

Authentication

Not required (Authentication is not required to exploit the vulnerability.)

Gained Access

None

Vulnerability Type(s)

Execute Code Overflow

CWE ID

119

– Products Affected By CVE-2006-2923

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	Application	Loudhush	Loudhush	1.3.6				Version Details Vulnerabilities

– Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions
Loudhush	Loudhush	1

– References For CVE-2006-2923

http://iaxclient.sourceforge.net/iaxcomm/ CONFIRM

http://secunia.com/advisories/20560 SECUNIA 20560

http://secunia.com/advisories/20567 SECUNIA 20567

http://secunia.com/advisories/20623 SECUNIA 20623

http://secunia.com/advisories/20900 SECUNIA 20900

http://sourceforge.net/project/shownotes.php?release_id=423099&group_id=131960 CONFIRM

https://web.archive.org/web/20140729171850/https://www.cvedetails.com/cve/CVE-2006-2923/

WIZ, Inc. EXHIBIT - 1090

WIZ, Inc. v. Orca Security LTD.

1/2

http://www.gentoo.org/security/en/glsa/glsa-200606-30.xml GENTOO GLSA-200606-30
http://www.coresecurity.com/common/showdoc.php?idx=548&idxseccion=10
http://www.vupen.com/english/advisories/2006/2286 VUPEN ADV-2006-2286
http://www.vupen.com/english/advisories/2006/2285 VUPEN ADV-2006-2285
http://www.vupen.com/english/advisories/2006/2284 VUPEN ADV-2006-2284
http://www.vupen.com/english/advisories/2006/2180 VUPEN ADV-2006-2180
http://www.securityfocus.com/archive/1/archive/1/436638/100/0/threaded BUGTRAQ 20060609 CORE-2006-0327: IAXclient truncated frames vulnerabilities
http://www.loudhush.ro/changelog.txt CONFIRM
http://xforce.iss.net/xforce/xfdb/27047 XF iaxclient-truncated-frame-bo(27047)
http://secunia.com/advisories/20466 SECUNIA 20466
http://www.securityfocus.com/bid/18307 BID 18307 IAXClient Multiple Truncated IAX Frames Remote Buffer Overflow Vulnerabilities <i>Release Date:2006-06-30</i>

– Metasploit Modules Related To CVE-2006-2923

There are not any metasploit modules related to this vulnerability (Please visit www.metasploit.com for more information)

[How does it work? Known limitations & technical details](#) [User agreement, disclaimer and privacy statement](#) [About & Contact](#) [Feedback](#)

CVE is a registered trademark of the MITRE Corporation and the authoritative source of CVE content is [MITRE's CVE web site](#). CWE is a registered trademark of the MITRE Corporation and the authoritative source of CWE content is [MITRE's CWE web site](#). OVAL is a registered trademark of The MITRE Corporation and the authoritative source of OVAL content is [MITRE's OVAL web site](#). Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.