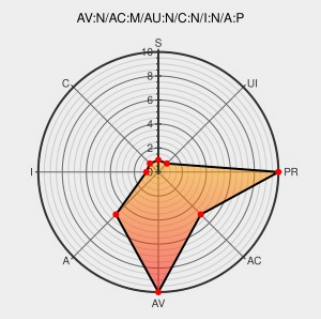
CVE-2010-1156

Published on: 04/16/2010 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:18 AM UTC

CVE-2010-1156

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



Certain versions of Irssi from Irssi contain the following vulnerability:

core/nicklist.c in Irssi before 0.8.15 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via vectors related to an attempted fuzzy nick match at the instant that a victim leaves a channel.

CVE-2010-1156 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
'[oss-security] CVE request: irssi 0.8.15' - MARC	marc.info text/html	MLIST [oss-security] 20100411 CVE request: irssi 0.8.15
Irssi - The client of the future	irssi.org text/html	CONFIRM irssi.org/news
Security Advisory SA39620 - Slackware update for irssi - Secunia	web.archive.org text/html	SECUNIA 39620
[SECURITY] Fedora 12 Update: irssi-0.8.15-1.fc12	lists.fedoraproject.org text/html	FEDORA FEDORA-2010-6629
'Re: [oss-security] CVE request: irssi 0.8.15' - MARC	marc.info text/html	MLIST [oss-security] 20100413 Re: CVE request: irssi 0.8.15
SecurityTracker.com Archives - Irssi Unspecified Bug Lets Remote Users Deny Service	securitytracker.com text/html	SECTRACK 1023845

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2010-1110
'Re: [oss-security] CVE request: irssi 0.8.15' - MARC	marc.info text/html	MLIST [oss-security] 20100412 Re: CVE request: irssi 0.8.15
No Description Provided	svn.irssi.org Inactive Link Not Archived	CONFIRM svn.irssi.org/cgi-bin/viewvc.cgi/irssi/trunk/src/core/nicklist.c?root=irssi&r1=4922&r2=5126
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:011	lists.opensuse.org text/html	SUSE SUSE-SR:2010:011
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2010-0987
'Re: [oss-security] CVE request: irssi 0.8.15' - MARC	marc.info text/html	MLIST [oss-security] 20100412 Re: CVE request: irssi 0.8.15
The Slackware Linux Project: Slackware Security Advisories	slackware.com text/html	SLACKWARE SSA:2010-116-01
USN-929-1: irssi vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-929-1
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF irssi-unspecified-dos(57791)
Fedora update for irssi - Advisories - Community	web.archive.org text/html	SECUNIA 39797
'[oss-security] Re: CVE request: irssi 0.8.15' - MARC	marc.info text/html	MLIST [oss-security] 20100413 Re: CVE request: irssi 0.8.15
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2010-1107
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Patch Vendor Advisory www.vupen.com text/html	VUPEN ADV-2010-0856
Irssi - The client of the future	irssi.org text/html	CONFIRM irssi.org/news/ChangeLog
irssi Denial of Service and SSL Hostname Verification Vulnerabilities - Advisories - Community	Vendor Advisory web.archive.org text/html	SECUNIA 39365

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Irssi	Irssi	0.8.0	All	All	All
Application	Irssi	Irssi	0.8.1	All	All	All

Application	lrssi	lrssi	0.8.10	All	All	All
Application	lrssi	lrssi	0.8.10	rc5	All	All
Application	lrssi	lrssi	0.8.10	rc6	All	All
Application	lrssi	lrssi	0.8.10	rc7	All	All
Application	lrssi	lrssi	0.8.10	rc8	All	All
Application	lrssi	lrssi	0.8.11	All	All	All
Application	lrssi	lrssi	0.8.11	rc1	All	All
Application	lrssi	lrssi	0.8.11	rc2	All	All
Application	lrssi	lrssi	0.8.12	All	All	All
Application	lrssi	lrssi	0.8.12	rc1	All	All
Application	lrssi	lrssi	0.8.13	All	All	All
Application	lrssi	lrssi	0.8.13	rc1	All	All
Application	lrssi	lrssi	0.8.14	All	All	All
Application	lrssi	lrssi	0.8.2	All	All	All
Application	lrssi	lrssi	0.8.3	All	All	All
Application	lrssi	lrssi	0.8.4	All	All	All
Application	lrssi	lrssi	0.8.5	All	All	All
Application	lrssi	lrssi	0.8.6	All	All	All
Application	lrssi	lrssi	0.8.7	All	All	All
Application	lrssi	lrssi	0.8.8	All	All	All
Application	lrssi	lrssi	0.8.9	All	All	All
Application	lrssi	lrssi	All	rc1	All	All
Application	lrssi	lrssi	0.8.0	All	All	All
Application	lrssi	lrssi	0.8.1	All	All	All
Application	lrssi	lrssi	0.8.10	All	All	All
Application	lrssi	lrssi	0.8.10	rc5	All	All
Application	lrssi	lrssi	0.8.10	rc6	All	All
Application	lrssi	lrssi	0.8.10	rc7	All	All
Application	lrssi	lrssi	0.8.10	rc8	All	All
Application	lrssi	lrssi	0.8.11	All	All	All
Application	lrssi	lrssi	0.8.11	rc1	All	All
Application	lrssi	lrssi	0.8.11	rc2	All	All
Application	lrssi	lrssi	0.8.12	All	All	All
Application	lrssi	lrssi	0.8.12	rc1	All	All
Application	lrssi	lrssi	0.8.13	All	All	All

Application	Irssi	Irssi	0.8.13	rc1	All	All
Application	Irssi	Irssi	0.8.14	All	All	All
Application	Irssi	Irssi	0.8.2	All	All	All
Application	Irssi	Irssi	0.8.3	All	All	All
Application	Irssi	Irssi	0.8.4	All	All	All
Application	Irssi	Irssi	0.8.5	All	All	All
Application	Irssi	Irssi	0.8.6	All	All	All
Application	Irssi	Irssi	0.8.7	All	All	All
Application	Irssi	Irssi	0.8.8	All	All	All
Application	Irssi	Irssi	0.8.9	All	All	All

cpe:2.3:a:irssi:irssi:0.8.0:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.1:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.10:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.10:rc5:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.10:rc6:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.10:rc7:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.10:rc8:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.11:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.11:rc1:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.11:rc2:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.12:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.12:rc1:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.13:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.13:rc1:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.14:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.2:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.3:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.4:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.5:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.6:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.7:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.8:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.9:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:*:rc1:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.0:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.1:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.10:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.10:rc5:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.10:rc6:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.10:rc7:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.10:rc8:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.11:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.11:rc1:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.11:rc2:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.12:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.12:rc1:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.13:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.13:rc1:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.14:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.2:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.3:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.4:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.5:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.6:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.7:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.8:*:*:*:*:*:*:*:

cpe:2.3:a:irssi:irssi:0.8.9:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID Next ID→

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