

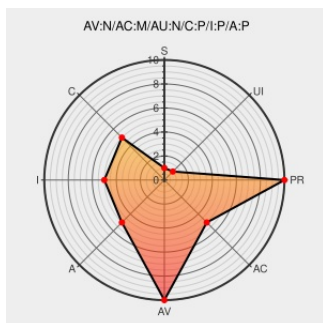


CVE-2010-1155

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

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

CVE-2010-1155

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Irssi](#) from [Irssi](#) contain the following vulnerability:

Irssi before 0.8.15, when SSL is used, does not verify that the server hostname matches a domain name in the subject's Common Name (CN) field or a Subject Alternative Name field of the X.509 certificate, which allows man-in-the-middle attackers to spoof IRC servers via an arbitrary certificate.

CVE-2010-1155 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

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](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[www.vupen.com](#)
[text/html](#)

[VUPEN ADV-2010-1110](#)

[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] 20100413 Re: CVE request: irssi 0.8.15
'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
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF irssi-hostname-mitm(57790)
USN-929-1: irssi vulnerabilities Ubuntu	www.ubuntu.com text/html	UBUNTU USN-929-1
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
Check if an SSL certificate matches the hostname of the server we are... · ensc/irssi-proxy@85bbc05 · GitHub	github.com text/html	CONFIRM github.com/ensc/irssi-proxy/commit/85bbc05b21678e80423815d2ef1dfe26208491ab
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

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	Irssi	Irssi	0.8.0	All	All	All
Application	Irssi	Irssi	0.8.1	All	All	All
Application	Irssi	Irssi	0.8.10	All	All	All
Application	Irssi	Irssi	0.8.10	rc5	All	All
Application	Irssi	Irssi	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	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	0.8.2	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 →](#)

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.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)