

# [NT] Chat Anywhere DoS

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0006.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 09/02/04

To: list@securiteam.com

Date: 2 Sep 2004 12:51:18 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Chat Anywhere DoS

---

## SUMMARY

<<http://www.lionmax.com/chatanywhere.htm>> Chat Anywhere is a "powerful chat server software for real-time chatting. With Chat Anywhere, you can easily design professional web-based chat rooms. You don't have to know any computer program language to use this software."

The chat server can be caused to crash by connecting fake users to it.

## DETAILS

Vulnerable Systems:

- \* Chat Anywhere version 2.72a

The chat server is unable to manage fake users. An attacker can crash the chat server and cause it to consume a lot of CPU resources. The CPU hogging effect is not limited to the server itself but propagates to all the real clients connected.

Exploit:

The following proof of concept is available from

<[http://www.autistici.org/fdonato/poc/ChatAnywhere\[272a\]DoS-poc.zip](http://www.autistici.org/fdonato/poc/ChatAnywhere[272a]DoS-poc.zip)>  
[http://www.autistici.org/fdonato/poc/ChatAnywhere\[272a\]DoS-poc.zip](http://www.autistici.org/fdonato/poc/ChatAnywhere[272a]DoS-poc.zip).

Securiteam: [NT] Chat Anywhere DoS

And from <<http://aluidgi.altervista.org/poc/chatanydos.zip>>  
<http://aluidgi.altervista.org/poc/chatanydos.zip>.

Vendor Status:

The bug was initially found on 4 Dec 2003 in the version 2.72, and reported to the vendor by Luigi Auriemma, but the vendor probably forgot to fix it. So the vendor was contacted for the same bug in the next version 2.72a. Now the vendor is planning to fix the bug in the next release. In the meantime it is recommended to add password protection to protect the chat room.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:fdonato@autistici.org>>  
Donato Ferrante.

=====

This bulletin is sent to members of the SecuriTeam mailing list.  
To unsubscribe from the list, send mail with an empty subject line and body to:  
[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)  
In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====  
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.  
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.