

[NT] Webbsyte Chat DoS Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0016.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 08/04/04

To: list@securiteam.com

Date: 4 Aug 2004 01:05:55 +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>

Webbsyte Chat DoS Vulnerability

SUMMARY

<<http://sourceforge.net/projects/wchat/>> Webbsyte Chat "lets you keep in touch with people all around the world".

Webbsyte char server is vulnerable to a denial of service vulnerability which is exhibited by a server crash that can be triggered by any remote attacker.

DETAILS

Vulnerable Systems:

* Webbsyte Chat version 0.9.0

The chat server doesn't correctly manage raw requests, in fact it will crash with the following error:

"Run-time error '40006':

Wrong protocol or connection state for the requested transaction or request"

What triggers the vulnerability are mere 40 simultaneous raw connections to the server. No more than 40 simulataneous connections are needed in order to bring down the server with the above mentioned error.

Securiteam: [NT] Webbsyte Chat DoS Vulnerability

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
In order to subscribe to the mailing list, simply forward this email to: 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.