

[NT] Buffer Overflow in WideChapter Browser

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0047.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/16/03

To: list@securiteam.com

Date: 16 Sep 2003 16:06:31 +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>

Buffer Overflow in WideChapter Browser

SUMMARY

<<http://www.widechapter.com>> WideChapter "is the most powerful multi Chapter multi tab web browser. WideChapter is a stable, fast, user-friendly browser. WideChapter gives each web site its own tab! WideChapter runs under Windows 98, Windows NT4, Windows ME, Windows 2000, and Windows XP and requires that IE to be installed. WideChapter is a standalone browser application that uses services provided by Microsoft Internet Explorer to navigate HTML. WideChapter currently requires Internet Explorer 5.5/above to be installed on the client computer".

It is possible to cause a buffer overflow in WideChapter Browser by causing it to initiate a long HTTP request. The overflow allows modification of the EIP pointer – allowing a malicious attacker to cause the program to execute arbitrary code.

DETAILS

Vendor Status:

The vendor has been informed, and they are fixing this bug.

Proof of concept exploit:

By embedding the following JavaScript into a web page: <

Securiteam: [NT] Buffer Overflow in WideChapter Browser

script>window.open([http://AAA.. \[Ax517\]](http://AAA.. [Ax517]))</script>, it is possible to cause the EIP to overwrite once a user visits the web page.

An exploit for Windows XP Home has created and is available for download from: <<http://www.elitehaven.net/wcexploit.zip>>
<http://www.elitehaven.net/wcexploit.zip>

ADDITIONAL INFORMATION

The information has been provided by <mailto:b_naamneh@hotmail.com> Bahaa Naamneh.

=====

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.