

# [VulnWatch] File Selection May Lead to Command Execution (GM#015-IE)

*Source:* <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2005-04/0023.html>

---

*From:* GreyMagic Security ([security\\_at\\_greymagic.com](mailto:security_at_greymagic.com))

*Date:* 04/19/05

To: <[vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)>

Date: Tue, 19 Apr 2005 17:30:39 +0200

GreyMagic Security Advisory GM#015-IE  
=====

By GreyMagic Software.  
19 Apr 2005.

Available in HTML format at  
<http://www.greymagic.com/security/advisories/gm015-ie/>.

Topic: File Selection May Lead to Command Execution.

Discovery date: 18 Jan 2005.

Affected applications:  
=====

- \* Windows Explorer on Windows 2000 Professional.
- \* Windows Explorer on Windows 2000 Server.
- \* Windows Explorer on Windows 2000 Advanced Server.

Note that any other application that uses the Web View DLL under Windows 2000 is affected as well.

Introduction:  
=====

Windows Explorer is used to navigate through the Windows file system by default.

Windows Explorer includes a preview pane (Web view), which displays information on some types of files when they become selected. The preview pane is enabled by default on all Windows 2000 systems.

The preview pane is implemented via an HTML resource file (in webvw.dll), which examines the currently selected file, reads its metadata and displays

## VulnWatch: [VulnWatch] File Selection May Lead to Command Execution (GM#015-IE)

useful information about it. Such information includes the file's size, attributes, modification date, author and more.

### Discussion:

=====

When the preview pane outputs the document's author name, it checks whether the name resembles an email address, and if so, transforms it into a 'mailto:' link in the pane.

The transformation into a link does not filter potentially dangerous characters and makes it possible to inject attributes into the link, which enables execution of arbitrary script commands.

Script commands that are injected in this manner will execute as soon as the malicious file is selected in Windows Explorer and will be executed in a trusted context, which means they will have the ability to perform any action the currently logged on user can perform. This includes reading, deleting and writing files, as well as executing arbitrary commands.

Notice that the malicious file does not need to be executed in order to activate the exploit, double-clicking is not required. The exploitation takes place as soon as the file is selected.

The code below is an excerpt from one of the vulnerable resources. In this instance 'safeData' has not been filtered properly, and may contain the apostrophe (') character, allowing for attribute termination in the resulting HTML:

```
text += "<p>" + title + ": <a href='mailto:" + safeData + "'>" + safeData +  
"</a>";
```

### Exploit:

=====

When setting the author field of a file (for example, a Word document) to the following value:

```
a@b' style='background-image:url(javascript:alert("Successful injection!"))'
```

Windows Explorer will display a message box as soon as the file is selected.

This vulnerability can also be exploited by directing the user to an attacker controlled SMB share, the user will then need to select the file in order to activate the exploit.

### Demonstration:

=====

GreyMagic has put together three proof-of-concept demonstrations:

## VulnWatch: [VulnWatch] File Selection May Lead to Command Execution (GM#015-IE)

- \* Simple: As shown in the exploit section, displays a simple message box when selected.
- \* Copy me: Automatically copies itself to the same folder when selected.
- \* Bo Selecta: Constantly renames itself when selected.

They may be accessed at

<http://security.greymagic.com/security/advisories/gm015-ie/>

Solution:

=====

Until a patch becomes available, disable the Web View by going to: Tools -> Folder Options -> Select 'Use Windows classic folders'.

Tested on:

=====

Windows Explorer / Windows 2000 Professional.  
Windows Explorer / Windows 2000 Server.  
Windows Explorer / Windows 2000 Advanced Server.

Disclaimer:

=====

The information in this security advisory and any of its demonstrations is provided "as is" without warranty of any kind.

Vulnerability details are provided strictly for educational and defensive purposes.

GreyMagic Software is not liable for any direct or indirect damages caused as a result of using the information or demonstrations provided in any part of this advisory.

- Copyright © 2005 GreyMagic Software.