

First Remote Code Execution Vulnerability affecting Microsoft Notepad

Secumania Security Group

<http://www.secumania.net>

edu (edu@secumania.net)

2010 March

Abstract

We are going to show you a little creativity; the process of triggering the first remote code execution vulnerability that affects Microsoft Notepad via innocent TXT documents!

We've heard so many times people saying "Notepad is too simple. It is impossible to find a code execution bug." Well, impossible is simply what has not yet been accomplished.

The vulnerability we are going to present you in this article, is actually not in the notepad itself, but in a component it loads. Of course the attack vector is an innocent txt file.

Important Note:

I take no responsibility of what you do with this information. Test it only in computers that you own or have the explicit permission to perform the tests.

1. Theoretical information

The MS HTML Help control ActiveX is prone to a remote CHM help file hijack vulnerability when applications invoke help. Multiple built-in applications are vulnerable to this. The impact of the vulnerability is the loading of the incorrect CHM help file when it resides in the same directory that the application invoking help starts in. The best attack vector I found for this, surprisingly is the safest and simplest Microsoft Windows built-in application: Microsoft Notepad.

Yes, the first remote code execution vulnerability involving the good old Notepad, and the vector as you are likely thinking of is an innocent TXT file, which can be opened in the local disk or in a remote NetBIOS share. Some user interaction is required though, specially if the file is invoked in a remote network share. The reason is (as Microsoft states) CHM files running in any security zone other than the Local machine doesn't work.

Well, this is partially true: In some situations there is a table of contents (*.hhc*) file in the CHM, and it contains the "local" parameter of an object tag pointing to a JavaScript URL. When the user clicks, the JavaScript URL is executed under the context of a local html file that HTML Help uses to display an error page (*res://ieframe.dll/navcancl.htm*). It means the script code is parsed in the context of the *local machine* security zone, thus arbitrary code can be executed. So, what does the user need to do in order to have arbitrary code executed? The answer depends whether the attack is performed locally or on a network-basis.

1) In a remote scenario

Double click a text file located in a remote NetBIOS share, proceed to press F1 key and then click on a topic (in the left pane of the HTML Help window)

2) In the local computer (*when eg. extracting files from a zip archive*)

Double click a text file and then press F1. This is enough to run arbitrary code, because the embedded HTML files are processed in the local machine security zone context, and is able, for example, to use the HTML Help ActiveX and the shortcut parameter to run arbitrary programs automatically.

Severity: *Medium-low / Medium*

Impact: *Arbitrary Code Execution*

2. The vector in practice

Two Proof-of-Concepts are provided. One that works on the local disk and the other one on a remote network share. Network shares can be automatically invoked by Internet Explorer, upon accessing a webpage.

You would place all the files in the root directory (**C:**). Put the start.htm in a web server and access it with IE. It will open a default share (**\\127.0.0.1\c\$**). All the code is executed having the above address as base, so if you are going to change stuff, edit all the files, else it won't work. You will need HTML Help Workshop to extract the files from the '**notepad.chm**' file and edit the script code in the '**notepad.hhc**' file. If all works fine, you should see command prompt and calc being executed.

System Affected:

Tested on Windows XP SP3 fully patched, Windows 2000 SP4. Windows Vista and 7 are not affected because they use a new help system.

Affected Applications:

Most windows applications that utilize the HTML Help control to display help to the user. This includes Paint, Image and Fax Viewer, Word Pad, Internet Explorer (any version), etc. But the problem with these applications is:

- a) Paint on XP doesn't have by default any type of file associated. On Windows 2000, bitmap images open in Paint by default so it can be a good vector on windows 2000.
- b) Image and Fax Viewer, this is a DLL loaded in Explorer.exe process which by default starts in the user's base dir (XP) so the only chance is placing a CHM in the user's base directory. It doesn't seem a good vector.
- c) Word pad. This application is forced to start in the "my documents" directory. It doesn't seem a good vector.
- d) Internet Explorer. This application is forced to start in the user's desktop directory. It doesn't seem a good vector.
- e) Notepad. It seems a good vector on both XP and 2000 windows platforms.

Copyright © 2006-2010 Secumania Security Group
The Author retains Full Rights