Race conditions in security dialogs

2011-10-16 02:34:45 by Southern

From www.squarefree.com

I discovered arbitrary code execution holes in Firefox, Internet Explorer, and Opera that involve human reaction time. One version of the attack works like this:

The secret word fills the blank in the sentence 'If ____ web developers would use alternate text correctly!' It is all lowercase.

The page contains a captcha displaying the word "only" and asks you to type the word to verify that you are a human. As soon as you type 'n', the site attempts to install software, resulting in a security dialog. When you type 'y' at the end of the word, you trigger the 'Yes' button in the dialog. I made a demo of this attack for Firefox and Mozilla.

Another form of the attack involves convincing the user to double-click a certain spot on the screen. This spot happens to be the location where the 'Yes' button will appear. The first click triggers the dialog; the second click lands on the 'Yes' button. I made a demo of this attack for Firefox and Mozilla.

more: squarefree