It rather involved being on the other side of this airtight hatchway: Local execution

devblogs.microsoft.com/oldnewthing/20071031-00

October 31, 2007

Raymond Chen

The security response team gets all sorts of reports, and a good number of them are from people who just get excited that they were able to do something unusual, even if it isn't a security vulnerability.

> Attached please find a security exploit in the ABC ActiveX control. If you save this Web page to a file and double-click it, it <does something that Web pages shouldn't be allowed to do>.

The security folks study the Web page and discover that it indeed uses the ABC ActiveX control and invokes a method that is not safe from untrusted script, say, delete a file. But the control is marked *not safe for scripting*. How can script execute it? More careful study shows that the *not safe for scripting* attribute is indeed being respected. Copying the page to a Web server and visiting it from Internet Explorer blocks the creation of the ActiveX object, as expected. The only reason the local Web page version works is that you copied the file to your computer and ran it from there. If you do that, it runs in the context of the local computer rather than an untrusted Web server. When this was pointed out to the person reporting the alleged vulnerability, the explanation was, "That's right. To use this exploit, you have to convince users to save the file to their computer and double-click it. I understand that there is a lot that would have to happen for this exploit to succeed, but it's still possible." Well, heck, if that's your M.O, then why bother with the Web page? You can do the same thing with a boring executable. "To use this exploit, you simply have to convince users to save the file to their computer and double-click it. I understand that there is a lot that would have to happen for this exploit to succeed, but it's still possible."

Saving the file to the local computer is the step that crossed the security boundary. And that's the step these people just waved their hands at. They're assuming they're on the other side of the airtight hatchway and then proclaiming, "Woo-hoo! I managed to sneak to the other side of the airtight hatchway!"

Raymond Chen

Follow