

Re: SUPER SPOOF DELUXE Re: [Full-Disclosure] Microsoft and Security

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2004-07/0001.html>

From: Thor Larholm (*thor_at_PIVX.COM*)

Date: 07/02/04

Date: Thu, 1 Jul 2004 18:00:07 -0700

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

> *From: Pavel Kankovsky [mailto:peak@argo.troja.mff.cuni.cz]*

> *If a script from site A can replace the contents of a frame
> within a document from site B then site A is able to violate
> the *integrity* of B's contents. This is unacceptable.*

A script from site A can only replace the contents of a window object within a frame from site B if site B is specifically opened through scripting from site A. Site A cannot interact with any window object that it has not created itself, it has to open a new window, wait for it to load and then load a new document in the frame inside this new window. It doesn't even know if you already have an existing browser window pointing at WindowsUpdate or your banking site because it didn't open those windows.

You have to look at the prerequisite attack scenario. You are surfing to some random site and out of nowhere it opens WellsFargo.com or WindowsUpdate. At this point you are thinking one of 2 things, either

"What the.. I didn't go to WindowsUpdate/WellsFargo .. Let me just close that window .. Damn popups"

or

"Hey how nice, WindowsUpdate/WellsFargo magically appeared in front of me and I didn't even intend to go there .. I was just surfing for porn .. Let me hurriedly download some stuff from there and give it my account details"

Thor

NTBugtraq Editor's Note:

NT-Bugtraq: Re: SUPER SPOOF DELUXE Re: [Full-Disclosure] Microsoft and Security

Want to reply to the person who sent this message? This list is configured such that just hitting reply is going to result in the message coming to the list, not to the individual who sent the message. This was done to help reduce the number of Out of Office messages posters received. So if you want to send a reply just to the poster, you'll have to copy their email address out of the message and place it in your TO: field.
