

Re: IE URL obfuscation

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-12/0040.html>

From: Russ (*Russ.Cooper_at_RC.ON.CA*)

Date: 12/11/03

Date: Thu, 11 Dec 2003 11:07:16 -0500

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

More than a few people have pointed out the potential ramifications of the %01 IE URL obfuscation issue. The most common concern is that because the bug allows an attacker to forge the information in the Address bar, attackers are going to use it to convince unsuspecting consumers to go to forged bank sites or other such sites the user trusts.

There is clearly the potential for this, but I'm not sure people have fully thought this issue out.

I'm asking these questions with the thought of requesting that Microsoft consider this an emergency issue.

At this point I am not convinced that it is such an important issue that we need Microsoft to rush a patch out. However, given the concern expressed by subscribers, I'd like to offer some of my thoughts on the real risks, and then ask you to take a poll with them in mind.

1. Consider the premise that an attacker sets up a duplicate site for BankX. Emails are sent out to unsuspecting consumers in the hopes of hitting customers of BankX;

Caveat:

a) Consumers must be using IE with Hotmail or a similar Browser-based email, or Outlook Express rather than Outlook. Outlook has so far shown to be resistant to accepting the malicious URL.

2. Assuming the criteria is met, consumer believes the contents of the email and clicks on a malicious link. It takes the consumer to the spoofed site where they're asked for, say, their BankX login information.

Caveats:

a) The spoofed BankX site probably won't be SSL. If the forger uses a home made cert, the consumer will be prompted arriving at the site that the certificate comes from a CA not trusted by them. If the forger uses a cert from a reputable CA, they will likely have to provide more information to the CA than they want to provide. In addition, moving the site around to avoid detection wouldn't be possible with a valid cert, otherwise the consumer would get another warning that the site didn't match the issuing cert criteria.

b) At least my bank, and probably many more, have sent messages to customers telling them not to click on any link in an email about the bank. Instead, the customer has been told to type the URL in themselves. Further, most people probably have their bank site in their favorites, so they could call it up from there instead of clicking on the email.

NT–Bugtraq: Re: IE URL obfuscation

3. Assume now the consumer is at the site, and presumably has not received any warnings thusfar. Some people have suggested that consumers then should look at the URL in the address bar to verify they are where they think they are. I contend that consumers are not likely to do this.

Caveats:

- a) There was sufficient social engineering in the email to convince them it was legitimate, otherwise they would never have clicked on the link in the first place.
- b) They are going to look at the web site contents to determine if its BankX. They will look for BankX logos, look to see if the page looks familiar, etc... and use that to determine if they're at the right place.
- c) I believe most consumers ask their bank sites to remember their bank card number or userID. Most such sites don't offer the opportunity to remember your password. If the site doesn't bring up their userID, or bank card number, in the login field they may get suspicious. Having to re–type a 9 digit bank card number when they normally have it presented to them gives them time to pause.
- d) Due to widespread media suggestions, they may, if they think about security at all, look for a lock at the bottom of the page and probably not see one. This alone won't stop them, but again, it may give them pause.
- e) I know many people who surf entirely based on favorites and search engines. They rarely, if ever, type a URL into the Address box. Such people often don't even have the address box showing, let alone look at it.

Summary

The most likely use of this vulnerability is to succeed in point #2 above, convincing the consumer the email message is valid. Hovering a mouse of malicious URLs displays the forged URL only. Since most consumers aren't going to look at the source of the email or the properties of a URL, the mouseover action is the only thing which might tip them off.

So how many more people are we going to convince? We've had scams involving fake display URLs versus the underlying URL for ages. Such URLs look, in email, just like this new malformed URL will. The only difference is that the address bar will also display the forged URL. Its always been possible to forge what is seen when a mouse hovers over a link.

What shows up in the address bar only happens after the user clicks the link. They've already accepted the social engineering at that point. If the link takes them to a malicious site, the site might immediately exploit an IE vulnerability. That the consumer might look at it and determine they're not where they thought they were supposed to be doesn't reduce their risk significantly. It may make them stop and not enter their login information, but if the site exploited them that would have already happened.

So, take my poll, tell me whether you think we need an emergency patch or not.

<http://ntbugtraq.ntadvice.com/default.asp?sid=1&pid=47&aid=83>

Cheers,

Russ – Surgeon General of TruSecure Corporation/NTBugtraq Editor

NTBugtraq subscribers save \$103.00 off the TICSA exam by using promo code "NT1003" when registering to take the TICSA exam at www.2test.com. Prove to your employer and peers that you have the knowledge and

Re: IE URL obfuscation

NT-Bugtraq: Re: IE URL obfuscation

abilities to be an active stakeholder in today's enterprise security.
Become TICSА certified www.trusecure.com/ticsa. Promotion expires
12/31/03 and cannot be used in combination with other offers.
