

Re: [VulnWatch] xp sp2 weaknesses

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2004-08/0020.html>

From: hellNbak (hellnbak_at_nmrc.org)

Date: 08/18/04

Date: Wed, 18 Aug 2004 14:05:50 -0500 (CDT)

To: "Richie B." <richie@NO-SPAM-HERE.com>

I have a couple comments on this paper.

"The command shell cmd.exe ignores the ZoneID of files"

The ZoneID "feature" was built into Windows Explorer. Not the command shell. So I can see why this would be ignored but I do agree with the author that this is a bug. The severity of it, in my opinion is quite low as I do not see a legitimate exploit path. Any script pushed to the system via the web or email would be marked with a ZoneID -- so how does the attacker get it to launch from the command prompt and not via explorer? He can't. Any remote execution will have to be pushed via the internet or an email -- meaning the ZoneIDs will be processed -- even if the first line of your script is `cmd /c` it won't work REMOTELY.

Now if you already have access to a command shell, or even local access to a machine then yes, you can definitely use this -- but if you already have that level of access.....blah blah best cough practices cough blah...

The attack vector outlined in the paper is as follows;

"Attack vector

Exploitation of this issue requires some user interaction -- at least as long as nobody comes up with a way to execute cmd.exe with parameters from within Outlook Express or Internet Explorer. But viruses doing "social engineering" are a common place by now. Bagle & Co asked users to enter a password to decode encrypted attachments. Therefore a virus author could create an e-mail worm like this:

Attached: access.gif

Hello,

attached you find the copy of your access data you requested. For security reasons, the file is scrambled and can only be viewed with cmd. To view it, save the

attached file, execute "cmd" from the start menu, drag&drop the file into the new window and hit return. cmd will descramble the file for you. "

Yes, this would work, providing your user is at a level that they understand how to actually launch a command prompt and providing that eventhough they have a slight clue on how to use their computer they are completely trusting of random emails that ask them to do this.... hmmm ok, maybe it is likely... ;-)

An easy solution to this are some simple best practices and host security measures that we all know every responsible IT organization uses right? *cough* *cough*

Issue 2;

"Windows Explorer caches the result of ZoneID lookups. If a file is overwritten, Explorer does not properly update this cached information to reflect the new ZoneID. This allows spoofing of trusted or non-existent ZoneIDs by overwriting files with trusted or non-existent ZoneIDs."

This one has interesting potential. But, as the author of the paper at Heise Security says; "Exploiting this issue requires the ability to overwrite existing files which have a trusted or non-existent ZoneID."

So I would consider this an issue that should be fixed but nothing that is super high risk yet. But once the next batch of IE flaws are disclosed this one may prove to be useful in variations of attacks we have seen before.

Overall, I think Microsoft is missing the boat with their response to these issues. Sure, right now they are low risk but there is a very likely chance that they can be leveraged later.

> *I haven't seen this report here yet.*

>

> *Flaws in SP2 security features*

> =====

>

> *1) The command shell cmd.exe ignores the ZoneID of files.*

> *2) Windows Explorer caches the result of ZoneID lookups. If a file is overwritten, Explorer does not properly update this cached information to reflect the new ZoneID. This allows spoofing of trusted or non-existent ZoneIDs by overwriting files with trusted or non-existent ZoneIDs.*

>

> *URL: <http://www.heise.de/security/artikel/50051>*

>

> *Cheers,*

>

> *Richie*

VulnWatch: Re: [VulnWatch] xp sp2 weaknesses

>