

Re: Microsoft and Security

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2004-06/0055.html>

From: Drew Copley (*dcopley_at_EEYE.COM*)

Date: 06/26/04

Date: Fri, 25 Jun 2004 15:40:42 -0700
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

> -----Original Message-----

> From: *http-equiv@excite.com [mailto:1@malware.com]*

> Sent: Friday, June 25, 2004 11:53 AM

> To: *bugtraq@securityfocus.com*

> Subject: Microsoft and Security

<snip>

> A vulnerability:

>

> [http://www.microsoft.com/technet/archive/community/columns/securi](http://www.microsoft.com/technet/archive/community/columns/security/essays/vulnrbl.mspx)

> [ty/essays/vulnrbl.mspx](http://www.microsoft.com/technet/archive/community/columns/securi)

>

> "A security vulnerability is a flaw in a product that makes it
> infeasible – even when using the product properly—to prevent an
> attacker from usurping privileges on the user's system,
> regulating its operation, compromising data on it, or assuming
> ungranted trust."

>

> what this gibberish? For the past 10 months the adobd.stream
> object is capable of writing files to the "all important
> customer's" computer. It has real world consequences. It rapes
> their computer. Does it fit into the gibberish custom
> definition. Plain and simple: "A security vulnerability is a
> flaw in a product that makes it infeasible". What kind of
> language is this. Reads like the financial department conjured
> it up.

LOL. Very well said...

I think the point is not being pushed home, though.

Ten month old vulnerability. Common denominator for all of these attacks. This latest one is using the same flaw we saw in one this past Spring. It is not the latest zero day, according to Symantec's latest paper.

NT-Bugtraq: Re: Microsoft and Security

In fact, even they state up front "to deploy the workaround for the adodb stream issue". Workaround.

This adodb stream issue – found by Jelmer – is unfixed by Microsoft.

I do not know why. I suppose it fits into their competitive "motif" somehow. They like to do these sorts of things.

It is a "bar lowering" vulnerability. Otherwise, these other attacks would not work. They never would have worked.

The workaround kill bits the activex. There is no reason for it, not enough of one. I think some IIS systems may use it. I am sure it provides some sort of piece in their competitive marketing strategy. But, kill the dying horse already.

Here is the free fix I made (ten months ago, re-released):
<http://www.eeye.com/html/research/alerts/AL20040610.html>

There is a reg file or an exe file. Whichever one prefers. We find the exe file is most handy for doing mass fixes across corporate networks.

Clue, people: Likely, you have been affected by one of these holes. If you are an administrator, your domain has almost surely been affected.

There is a huge market for identities. Do not be naive.

>
> *Disabling scripting won't solve it. Putting sites in one of the*
> *myriad of "zones" won't solve it. Internet Explorer can*
> *trivially be fooled into operating in the less than secure so-*
> *called "intranet zone" and it can be guided there remotely.*
>
> *What's happening here. Where is the Microsoft representative*
> *explaining all of this to the shareholders and "customers" they*
> *so dearly wish to protect. This is unacceptable. Someone must*
> *be held accountable.*
>
>
> --
> <http://www.malware.com>
>
>
>
>
>
>
>

NT-Bugtraq: Re: Microsoft and Security

NTBugtraq Editor's Note:

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.
