

Re: On classifying attacks

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2005-07/0284.html>

From: James Longstreet (jlongs2_at_uic.edu)

Date: 07/18/05

Date: Mon, 18 Jul 2005 10:49:00 -0500 (CDT)

To: Derek Martin <code@pizzashack.org>

On Sat, 16 Jul 2005, Derek Martin wrote:

- > *It seems to me your statement can't be correct, because this is ALWAYS*
- > *the case. A local exploit requires that a local user run an*
- > *executable. A remote exploit requires that a local user run an*
- > *executable, even if that is accomplished merely by booting the system.*
- > *All exploits require running code, and code doesn't magically start*
- > *itself... Running code is required, because it is the very running*
- > *code which is being exploited.*

Yes, but a trojan requires a user to run a program, not open a file. JPEGs are an image format, not an executable format. Opening one should display the image, not run arbitrary code.

- > *I think this is also not the case. To exploit essentially means to*
- > *use. These attacks USE the users' trust of e-mail in order to USE a*
- > *bug to gain access to USE the system for his own purposes... That*
- > *certainly seems like an exploit to me.*

But it's not a bug. A computer that runs an executable when it is double-clicked does not have a vulnerability.

Example:

All Unix systems are "vulnerable" to loss of data through the following exploit: an attacker sends the string "rm -rf /" through email. If the system administrator gives this string to his shell running as root, all data on the system will be lost.

- > *We disagree here. The vulnerability is neither truly remote nor*
- > *local, in the normal senses as we have defined them here. It is a*
- > *different kind of vulnerability altogether. The vulnerability is one*
- > *to automatically triggering trojan horses.... Just as in the case of*
- > *the fabled Trojan Horse, there is no vulnerability at all until the*
- > *local users make a decision to trust something (data in this case,*
- > *rather than a hollowed out horse-shaped monument) from an outside*
- > *source. In this case, the trust is given implicitly rather than*

SecurityFocus Bugtraq: Re: On classifying attacks

- > *explicitly. This is no different than if I handed you a disk, told*
- > *you to run the program on the disk, and you did so -- resulting in the*
- > *destruction of your hard drive. Would you call this a remote*
- > *vulnerability? Of course not. But the mechanism is exactly the*
- > *same... except that some of the minor details are different.*

It's completely different. If you gave me a program on a disk, I wouldn't run it, because I know that programs that I run can do whatever they want on my system. That's not because of a bug, it's because that's what a computer does -- run programs.

- > *The only difference is the medium used to deliver the trojan horse is*
- > *a network instead of a disk, and it is slightly more automated,*
- > *because you are prone to automatically view the data out of habit. If*
- > *I did hand you a disk and tell you to run the program on it, you would*
- > *probably be a lot more wary of doing so than you would of reading your*
- > *e-mail, wouldn't you? Especially if you don't know me very well. But*
- > *if you were dumb enough to do so, would you call this a remote*
- > *exploit? What if I gave you a disk that had an Excel spreadsheet on*
- > *it, which contained data designed to take over your system using a bug*
- > *in excel... Is this a remote exploit? I don't think so. Now I use*
- > *the same excel spreadsheet, but I send it to you in e-mail instead of*
- > *giving it to you on a disk. In all cases, I have given the data to*
- > *you. In all cases, there is no exploit at all, until you, the local*
- > *user, decides to trust the data, and run broken code against it. The*
- > *only difference is the specific delivery mechanism, and the fact that*
- > *the average user implicitly trusts data received in e-mail. Because*
- > *really, what choice do they have?*

If you gave me an Excel spreadsheet on disk, I would expect to be able to open it and see a spreadsheet. I am allowing you to display a spreadsheet on my system, not to run arbitrary code. If there was a bug in Excel, you would be able to exploit my legitimate trust in Excel to run arbitrary code.

If you gave me a program on disk and I ran it, I am giving you permission to run arbitrary code on my system. Therefore, there is no bug. The blame lies solely on me, not on my operating system, computer, or the program itself.

- > *But this is still not a remote vulnerability. It is a user trust*
- > *vulnerability, as you said yourself. And it is a vulnerability (or*
- > *susceptibility) to trojan horse data. The fact that the data just*
- > *happens to come in via a network is largely irrelevant. A remote user*
- > *can, IN NO WAY, effect an exploit against this kind of vulnerability*
- > *merely by his own action. This exploit can not happen unless you, the*
- > *local user, do it for him. This is the essential reason why it is not*
- > *a remote vulnerability.*

Yes, but opening an untrusted image file, for example, is a legitimate use case. I would assume that almost all of us do so multiple times a day.

SecurityFocus Bugtraq: Re: On classifying attacks

Trusting a program whose job is to open JPEG files to do so is not a vulnerability.

> *Absolutely they should. But the fact that they DO trust it when it is*
> *not worthy of their trust does not make this a remote vulnerability.*

Your logic is flawed, though. Even if we agree to disagree on whether or not opening an untrusted data file is a trust issue or not, what makes it a remote vulnerability is the fact that the attacker does not need privileges on the system. Perhaps, you say, you are giving him privileges by opening his data file. But you are only giving him privileges to open that file, not to run arbitrary code.