

Re: Russ Cooper's AusCERT Presentation on MS Security Bulletins

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2004-06/0011.html>

From: Jake (jake_at_NTHELP.ORG)

Date: 06/04/04

Date: Thu, 3 Jun 2004 19:20:46 -0400

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Resending. This can go to the list.

Russ,

What is it that you would like Microsoft to do? It's a simple question. However, there is no simple answer and there never will be. As an MVP, Microsoft asks me ALL the time for my opinion of there products, services, and goals. Every MVP I have met has always been very frank with Microsoft and one of the top suggestions is "security". What is security? Patches? Firewalls? Built-in? Third-Party? How does the U.S. Navy secure an aircraft carrier? An aircraft carrier is NEVER left alone out there at sea. It takes teamwork. My point is this, Microsoft's Security Push can not be just patches, there has to be other pieces of the "team". The fact that newer releases of their products are now configured differently in a "locked-down" mode is a HUGE push for security. Something that I think you are minimizing.

Quote: "I stressed that, IMO, far too much effort is being placed on patching IE vulnerabilities. To the best of my knowledge, only 2 wide-spread attacks have occurred involving IE vulnerabilities, yet there have been at least 83 vulnerabilities patched for IE. Clearly a lot of effort is being spent patching vulnerabilities which have not resulted in exploits, IMO, a large waste of Corporate resources."

A waste of resources? How so? This statement has me completely baffled. Would you rather them NOT patch and wait for an exploit before reviewing and patching the software? If the security push is to detect failures BEFORE they happen, WHY are you considering it a waste of time when they do as they say they would?

NT-Bugtraq: Re: Russ Cooper's AusCERT Presentation on MS Security Bulletins

A final note, do you think that the guys reviewing the code for older apps/products are the same ones that wrote the apps/products? Well, for the most part, they're not. What does this mean? Learning curves, patience, and lot's of time. Vulnerabilities are going to affect all versions (nt4 through win2k3) because, "If it ain't broke, don't fix it." So now that the "Big Push" has begun, they've started finding vulnerabilities, and as they test and test and test and test... they are finding that things weren't broken and never fixed. So now they are being fixed, and they are being fixed retroactively. Is that not a sign that Microsoft is trying?

Jake

Microsoft MVP

>> *Windows Server > IIS*

<http://www.nthelp.org>

<http://www.computershowoff.com>

-----Original Message-----

From: Windows NTBugtraq Mailing List

[mailto:NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM] On Behalf Of Russ

Sent: Wednesday, June 02, 2004 1:43 PM

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Subject: Russ Cooper's AusCERT Presentation on MS Security Bulletins

<SNIPPED FOR SPACE>

Patch Automation v6.0 by Mobile Automation, Inc. allows you to quickly identify and fix all PC's that are exposed to the Sasser worm! Our solution provides quick and seamless discovery and deployment of all your PC computer's Microsoft security patching needs. Regardless of where you're PC's reside (inside the LAN, at home or on the road), Patch Automation gets the job done. Contact us to learn about our free 30-day trial version at 800-344-1150 or visit our website at

<<http://www.patchautomation.com>>
