

microsoft.public.windows.server.sbs: << SBS News of the Week August 8, 2004>>

<< SBS News of the Week August 8, 2004>>

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2004-08/2801.html>

From: Susan Bradley, CPA aka Ebitz – SBS Rocks [MVP] (*sbradcpa_at_pacbell.net*)

Date: 08/09/04

Date: Sun, 08 Aug 2004 23:51:55 -0700

The BIG NEWS

XP sp2 released to manufacturing

Channel 9 gives a demo of XP sp2

<http://channel9.msdn.com/ShowPost.aspx?PostID=9328>

What's the BIG news for SBSers?

We can enable the firewall on those SP2s "INSIDE" the network.

SBSized info for XP sp2:

<http://msmvps.com/bradley/archive/2004/08/07/11400.aspx>

Why would we want this? Defense in depth. Yes you already have ISA and RRAS firewall on the outside but you are a bit "squishy" on the inside.

This helps to limit those ports that you have exposed even internally.

We need two patches to enable the firewall in SBS 2k3

<http://www.microsoft.com/downloads/details.aspx?familyid=d70097c2-4317-40e0-b7da-feb52c6b6386>

Then you need this which WILL BE ON the download site [but just not yet ... be patient.. just make sure you dont' install the SBS gpo patch

until you have ONE machine on XPsp2

842933 – "The following entry in the [strings] section is too long and has been truncated" error message when you try to modify or to view GPOs in Windows Server 2003, Windows XP, or Windows 2000:

<http://support.microsoft.com/?kbid=842933>

Kevin's song of the week

<news://msnews.microsoft.com/#VR8MiWfEHA.2468@TK2MSFTNGP12.phx.gbl>

Chad shares a resolution to the OWA timeout issue

<news://msnews.microsoft.com/#1ODazcfEHA.1356@TK2MSFTNGP09.phx.gbl>

Michael Jenkin shares his Malware cleaner tool info
Spyware is getting bad.....:

<< SBS News of the Week August 8, 2004>>

microsoft.public.windows.server.sbs: << SBS News of the Week August 8, 2004>>

<http://msmvps.com/bradley/archive/2004/08/08/11469.aspx>

SMBnation is COMING UP FAST FOLKS!!!!

<http://www.smbnation.com>

883786 – Support WebCast: Deploying and licensing Microsoft Windows Small Business Server 2003:

<http://support.microsoft.com/default.aspx?scid=kb:en-us:883786>

Tuesday, August 17, 2004: 2:00 PM Pacific time (Greenwich mean time – 7 hours)

Are you thinking about deploying your first server? Are you upgrading to Microsoft Windows Small Business Server 2003? This Support WebCast talks about Windows Small Business Server 2003, an integrated, easy-to-use, affordable network solution for small businesses. In this session, you will learn how to select the right technology to meet your business requirements. Learn how to avoid common mistakes when implementing a first server or upgrading to Windows Small Business Server 2003. Hear about tips and tricks for easily deploying Small Business Server 2003. Hear the answers to frequently asked questions about licensing, product features, and more.

Want SBS whitepapers? Here's a listing of recent whitepapers on the Microsoft site.

<http://msmvps.com/bradley/archive/2004/08/08/11450.aspx>

Migrating from a Peer-to-Peer Network to a Windows Small Business Server 2003 Network

Deploying Windows 2000 Server Terminal Server to Host User Desktops in a Windows Small Business Server 2003 Environment

Installing and Securing Microsoft Small Business Manager 7.5 on Microsoft Windows Small Business Server 2003

Download this Connecting Mobile and Remote Users document

Download this Windows Small Business Server 2003 Feature Comparison Guide document

Download this Installing and Securing Microsoft CRM 1.2 on a Windows Small Business Server 2003 Network document

Windows XP Service Pack 2 and Windows Small Business Server

Watch out for Trend and net use drives after SP2

<news://msnews.microsoft.com/eXOmAhOfEHA.3612@TK2MSFTNGP12.phx.gbl>

<< SBS News of the Week August 8, 2004>>

Thanks Frank for that heads up!

In other news

Phone spam misery looms Stateside

A little-noticed Bill before the Senate will ensure daily misery for US cellphone users, thanks to the inattentiveness of telecomms regulator the FCC. This week the FCC ruled against spam sent to mobile users that originates from email addresses. The regulator believes that the 1991 Telephone Consumer Protection Act (TCPA) already regulates SMS text messages, and that's good enough. But a new bill, S.2603, passed by Congress (as HR.4600) two weeks ago, drives a horse and cart through the TCPA. The bill was approved by the House's Commerce, Science and Transportation Committee and will be considered by the floor.

http://www.theregister.co.uk/2004/08/06/junk_fax_sms_ok/

STATEMENT BY NY AG REGARDING FCC DECISION

http://www.oag.state.ny.us/press/2004/aug/aug5a_04.html

Lawyer sues Yahoo over message-board insults

A Californian who objects to personal attacks made by posters to Yahoo's message boards is attempting to launch a class-action lawsuit against the company. A California lawyer who has waged an ongoing battle with Yahoo over personal attacks made against him on Yahoo message boards has filed a proposed class-action lawsuit against the company.

<http://news.zdnet.co.uk/business/legal/0,39020651,39162798,00.htm>

'Stealing songs is wrong' lessons head for UK schools

At the beginning of last month the British Government launched a "Music Manifesto" to promote music in schools. But already this typically Blairite bundle of good intentions is being hijacked (with not a little cooperation from the minders in Whitehall) in order to inflict copyright lessons on schoolchildren, from pre-school onwards.

http://www.theregister.co.uk/2004/08/05/uk_school_copyright_lessons/

Windows security update ready to go

Microsoft on Friday wrapped up development on a long-awaited security update to Windows XP, paving the way for businesses and consumers

to upgrade in the coming days and months. The company said it has released Windows XP Service Pack 2 to manufacturing, following a series of delays. Microsoft will make the free update available via download and via CD, but it is recommending that customers turn on Windows' automatic upgrade feature and get the update that way.

http://zdnet.com.com/2100-1104_2-5300317.html

<http://www.msnbc.msn.com/id/5610539/>

<http://computerworld.com/softwaretopics/os/windows/story/0.10801.95101.00.html?from=homeheads>

Windows XP SP2 'Released to Manufacturing'

http://www.newsfactor.com/story.xhtml?story_title=Windows-XP-SP---Released-to-Manufacturing-&story_id=20

Mozilla, Opera Plug Security Holes

The Mozilla Foundation and Opera Software ASA have released updates to their Web browsers to fix a series of security vulnerabilities. Mozilla on Wednesday posted new versions of its Firefox browser, Thunderbird e-mail client and Mozilla suite that provide fixes to three issues. They include a newly reported critical vulnerability affecting multiple vendors' software that uses the library for the Portable Networks Graphic (PNG) image format.

<http://www.eweek.com/article2/0.1759.1632120.00.asp>

Images open door to attackers

<http://news.zdnet.co.uk/0.39020330.39162797.00.htm>

Yahoo's Anti-Spy toolbar feature buggy

Yahoo on Friday confirmed that its recently released toolbar has mistakenly linked an alleged spyware program with a product that has nothing to do with the application in question. A company representative said late Friday that its toolbar's Anti-Spy feature incorrectly identified alleged "hijacker" software known as SearchCentrix as being bundled with Claria's Gator eWallet product, which is designed to manage usernames and passwords. Hijacking programs redirect search results or tamper with browser settings, according to Yahoo.

http://news.com.com/Yahoo%27s+Anti-Spy+toolbar+feature+buggy/2100-1024_3-5300761.html

Security Cavities Ail Bluetooth

Serious flaws discovered in Bluetooth technology used in mobile phones can let an attacker remotely download contact information from victims' address books, read their calendar appointments or peruse text messages on their phones to conduct corporate

espionage. An attacker could even plant phony text messages in a phone's memory, or turn the phone sitting in a victim's pocket or on a restaurant table top into a listening device to pick up private conversations in the phone's vicinity. Most types of attacks could be conducted without leaving a trace.

<http://www.wired.com/news/privacy/0,1848,64463,00.html>

Can you hack the vote?

A \$10,000 challenge is at stake. Electronic voting systems have drawn fire from courts, lawmakers and citizens groups -- and now they're under attack by hackers. It's an organized assault, too. E-voting technology expert Rebecca Mercuri, a Harvard research fellow who has been outspoken in her opposition to such systems, has issued a "Hack the Vote" challenge, trying to illustrate what she calls the systems' unreliability and vulnerability.

<http://computerworld.com/governmenttopics/government/story/0,10801,95096,00.html>

Small security firm puts spotlight on big vendor bugs
Research company says it has discovered 67 undisclosed vulnerabilities in major vendors' software News earlier this week that Oracle Corp. was sitting on patches for 34 undisclosed vulnerabilities in its database software may have come as a surprise to some, but not to David Litchfield, the researcher who discovered the holes. "In general, bugs are getting harder to find but in some people's software you don't have to look very hard to find bugs, they just fall apart in your hands ... like Oracle's," Litchfield said in an interview Thursday.

http://www.infoworld.com/article/04/08/06/HNsecurityspotlight_1.html

Online data a gold mine for terrorists
IT's high-alert response overlooks corporate sites
The widespread availability of sensitive information on corporate Web sites appears to have been largely overlooked by IT and security managers responding this week to the Department of Homeland Security's warning of a heightened terrorist threat against the financial services sector.

<http://computerworld.com/securitytopics/security/story/0,10801,95098,00.html>

Wardriving guilty plea in Lowe's wi-fi case
In what prosecutors say is likely the first criminal conviction for wardriving in the U.S., a Michigan man plead guilty Wednesday to a federal misdemeanor for using the Internet through an open wi-fi access point at a Lowe's home improvement store in suburban

Detroit. Paul Timmins, 23, pleaded guilty to a single count of unauthorized access to a protected computer. He was cleared of more serious charges of participating in a scheme organized by his roommate and another man to later use the wireless network to hack into Lowe's computers and siphon credit card numbers.

<http://www.securityfocus.com/news/9281>

Image flaw pierces PC security

Six vulnerabilities in an open-source image format could allow intruders to compromise computers running Linux and may allow attacks against Windows PCs as well as Macs running OS X. The security issues appear in a library supporting the portable network graphics (PNG) format, used widely by programs such as the Mozilla and Opera browsers and various e-mail clients. The most critical issue, a memory problem known as a buffer overflow, could allow specially created PNG graphics to execute a malicious program when the application loads the image.

http://zdnet.com.com/2100-1105_2-5298999.html

http://news.com.com/Image+flaw+pierces+PC+security/2100-1002_3-5298999.html

Feds seek a few good hackers

Attention, hackers: Uncle Sam wants you. And hackers are answering the call, or at least listening. A well-attended session at the recent Defcon 12 hackers' conference was "Meet the Feds," a recruitment presentation by a group of federal cybercrime law enforcement agents, who fielded questions from would-be cybercops.

<http://computerworld.com/securitytopics/security/story/0,10801,95054,00.html>

FBI publishes computer crime and security stats

Every year for the past nine years, the Computer Security Institute and the FBI undertake a computer crime and security survey among companies and institutions in the US. These surveys provide interesting insights into the level of computer crime being experienced by companies, as well as how they are responding to security breaches.

http://www.theregister.co.uk/2004/08/05/fbi_security_stats/

Biggest ever Windows upgrade gives security boost

Almost since the day Microsoft Corp. released its Windows XP computer operating system nearly three years ago, it has been a favorite target of hackers and critics eager to stress its numerous security shortcomings. Now, more than two years after promising to do something about it, Microsoft is about to release the biggest update ever for

Windows. The free upgrade is designed to make users safer from cyberattacks by sealing entries to viruses, better protecting personal data and fending off spyware.

<http://www.securityfocus.com/news/9279>

Windows security update delayed again

<http://www.msnbc.msn.com/id/5610539/>

Microsoft to begin shipping major update to Windows

http://www.usatoday.com/tech/techinvestor/techcorporatenews/2004-08-05-sp2-nears-drop_x.htm

Oracle 'sitting on security fixes'

Database giant Oracle has been censured by a leading security expert for sitting on fixes to defend against a wide variety of security vulnerabilities affecting its database software. UK-based Next Generation Security Software (NGS Software) has identified 34 security vulnerabilities affecting various versions of Oracle's database software. Around half these flaws affect the latest version of Oracle's database software, 10g. At least one of these bugs could be exploited to give attackers remote access to corporate database servers without a user ID or password.

http://www.theregister.co.uk/2004/08/05/oracle_security_flap/

What's in a worm's name?

It's not easy naming worms. Antivirus researchers originally identified a recent security attack as a variant of MyDoom – but now think it's actually related to a different piece of malware. When security experts first detected a mass-mailing worm that uses Yahoo's People Search engine to harvest email addresses, they assumed it was a new variant of MyDoom, which a week earlier had attacked a number of search engines for the same purpose.

<http://news.zdnet.co.uk/internet/0,39020369,39162715,00.htm>

Onion Routing Averts Prying Eyes

Computer programmers are modifying a communications system, originally developed by the U.S. Naval Research Lab, to help Internet users surf the Web anonymously and shield their online activities from corporate or government eyes. The system is based on a concept called onion routing. It works like this: Messages, or packets of information, are sent through a distributed network of randomly selected servers, or nodes, each of which knows only its predecessor and successor. Messages flowing through this network are unwrapped by a symmetric encryption key at each server that peels off one layer and

reveals instructions for the next downstream node.

<http://www.wired.com/news/privacy/0,1848,64464,00.html>

Easy VoIP wiretaps coming soon

Virtually everything done via TCP/IP, with the (for now) exception of instant messaging, is on its way to becoming wiretap-friendly, thanks to a tentative 5-0 decision by the US Federal Communications Commission (FCC) on Wednesday. Thanks to relentless lobbying and fear-mongering by law enforcement outfits and the companies that sell surveillance equipment to them, all broadband communications, including VoIP, will have to be modified to allow the Feds to patch in easily and immediately, in order to comply with the 1994 Communications Assistance to Law Enforcement Act (CALEA).

<http://www.securityfocus.com/news/9277>

You are still the weakest security link

Yet again staff have been identified as the biggest security threat to business IT systems, in a survey released today. The poll of 1,240 British businesses found employee misuse of technology topping the reasons for security breaches, with 50 per cent of businesses having problems. The second highest cause, at 45 per cent, was poorly updated antivirus software.

<http://www.vnunet.com/news/1157129>

Bosses finger workers for virus attacks

http://www.theregister.co.uk/2004/08/05/iod_sme_security/

Don't Toss That Personal Firewall

The new firewall in Windows XP Service Pack 2 is not by any means the most important security advance in the service pack. Other changes, principally locking down the My Computer zone in Internet Explorer, will have more profound implications for security of the average system. But it's not unimportant.

http://story.news.yahoo.com/news?tmpl=story&cid=1738&ncid=1209&e=2&u=/zd/20040805/tc_zd/132874

--
<http://www.sbslinks.com/really.htm>