

# The Small Office Solutions Newsletter



Ronald L. Herold, Ph.D.

Local and Wide Area Networks  
e-Commerce and Custom Applications  
e-mail and WEB Presence

3612 Hummer Road, Annandale, VA 22003  
Tel: (703) 573-2222 Fax: (703) 573-2263  
E-mail: ronsolve@rrr.org Web: www.rrr.org

May 14, 2008

## In This Issue

- The Last Days to Buy XP
- XP Support
- XP SP3
- Computer Emergency Readiness Team (CERT)
- And I thought it was just my Environment
- Microsoft – NEXTGEN
- Drive by Internet Infections
- Security Updates

## The Last Days to Buy XP



Just a reminder that Microsoft will no longer all the sales of Windows XP after June 30<sup>th</sup>, 2008. You will only be able to purchase Vista on a new machine. I am going to presume that also means that you will not be able to buy Vista with downgrade licenses – either. [More on downgrade licenses in a moment]. Therefore – if you have a need for new machines – and have not tested XP to operate with all your

applications - then this is either the time to buy a Vista machine and verify that it works with all your applications – or stock up on XP workstations.

Downgrade licenses were a ‘temptation’ by Microsoft go get copies of Vista sold. In essence – you could buy a Vista license with your new PC and install XP. It would be interesting to note how Microsoft counted those sales – as XP or Vista – or both? To obtain the downgrade license – you must either purchase Vista Business or Ultimate either of which downgrades to XP Pro. In most cases – the XP is being preloaded on the workstation (no idea how you reload it if the hard drive crashes) and Vista Disks are sent with the workstation so that when you are ready to upgrade to Vista – you can. You may have to do some searching on the vendor web site for this option. For example, Dell calls it, “Genuine Windows Vista® Business Bonus - XP Pro preinstalled”. Each vendor will have their own notation.

## XP Support

Users running SP3 will be able to receive Microsoft's mainstream support until April 14, 2009, and extended support until April 8, 2014. Extended support is probably billable. You should note that it says – running XP SP3. If you are still on XP SP2 – then you will probably have to upgrade to get support.

## XP SP3

XP Service Pack 3 is out and now is being automatically downloaded during software updates.

There are some known (and I am sure more – yet to be discovered) issues. Here are two of the experienced issues:

1. Continuous reboots after its install or no boot at all. This appears to be something related to AMD processors - but it's not fully investigated.
2. Internet Explorer 7 (IE7) is installed and IS NOT removable. Make sure you have tested your major interfaces with IE7 before installing XP SP3. Remember - many programs that do not directly interface with the Internet use IE's modules for display, search and other features. So - it's not just the Internet you need be concerned with.

Users who experience problems installing XP SP3 can get free tech support from Microsoft at (866) 234-6020. I believe that is INSTALLATION support - not application support.

## Computer Emergency Readiness Team (CERT)



The Computer Emergency Readiness Team (CERT) is a government funded research effort designed for administrators to assist them in keeping your computers secure. CERT is located at Carnegie-Mellon University in Pittsburgh Pennsylvania (my Alma Mata) and includes some of the best computer scientists in the country. CERT can be found on the Internet at <http://cert.org>.

My reason for including information about CERT is to demonstrate a few points:

1. Microsoft isn't the only company with products with a slew of vulnerabilities
2. Many vulnerabilities have been known for a very long time – and still rank high in the list of frequently exploited vulnerabilities.

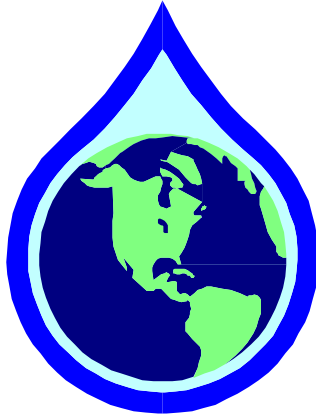
To show that Microsoft isn't the only company – take a look at <http://www.kb.cert.org/vuls/>. There you will find the 10 most recent vulnerabilities. Microsoft is only responsible for 2 out of 10.

Looking at <http://www.kb.cert.org/vuls/bymetric?open&start=1&count=20> provides a list of the 20 most severe vulnerabilities. The interesting fact is that since these are still listed – many locations have not fixed the vulnerabilities.

My point is that there are a non-stop list of vulnerabilities and that many sites are not doing the prudent process of managing vulnerability prevention.

That is why I am recommending that your organization do what you can for your office staff to keep them protected from not only Microsoft vulnerabilities but other web servers, switches and equipment to which you might surf or otherwise interact. The prudent approach is to take action at your site. One way to do this is by use of the **Content Control Trafficker (CCT)** that I described in detail in the March newsletter. It assists by recognizing threats and limiting the enthusiastic web surfer or voracious email reader from their interaction with these traps.

**And I thought it was just my Environment**



When I first established the **Content Control Trafficker** (CCT) at my office, I saw an enormous positive filtering effect to my incoming email. I thought that my environment was somehow unique because of my public involvement with the Internet. By contrast, I had expected that the effectiveness for the CCT would be somewhat less dramatic for my customers. Clearly, I was wrong as the data that follows shows.

For the week of May 6 to 13, I have tabularized the results from a few of my customers who use the CCT. The customer types are listed on the top with two columns given to each customer. The first is an absolute number of emails and the second is a percentage relative to the number of emails scanned.

Looking at the Small Association columns, there are 81,421 emails scanned in a 1 week period of which 63,507 are rejected by the sole criteria of coming from DNS addresses of known spammers. This is the row marked DNSBL. That represents 78% of the incoming traffic. Another 17,107 are recognized as SPAM as marked by the row label SPAM. That is 21.01% of the total number of messages. The remaining 807 or .99% are passed as valid messages as indicated by the row marked Passed.

In reviewing the various organizations – you can see that the largest number of rejected

	Small Association		Large Association		Medium Indust Corp		Small Svcs Corp		RRR	
Scanned	81421	100.00%	321538	100.00%	156753	100.00%	21455	100.00%	68917	100.00%
DNSBL	63507	78.00%	293722	91.35%	145206	92.63%	19500	90.89%	64974	94.28%
SPAM	17107	21.01%	22930	7.13%	9253	5.90%	1177	5.49%	2363	3.43%
Passed	807	<b>0.99%</b>	4886	<b>1.52%</b>	2294	<b>1.46%</b>	778	<b>3.63%</b>	1581	<b>2.29%</b>

emails come from the DNS Black List (DNSBL) of known spammers. In general only 1 to 4% of the emails are permitted to reach your company's the inbox.

Besides offering your employees many less SPAM filled emails to read or delete, by using CCT there is a side benefit. Your server doesn't have to 'deal' with an email until the CCT has determined that it doesn't belong to the DNSBL and is most likely not SPAM. A worst case scenario demonstrates a lowering of your server's requirement to process emails by 94%. In some cases – it can be as great as 99%. As our internal networks become more and more loaded – yet we retain the same server hardware and switching within our

offices, unloading the server of tasks that are not necessary will improve overall system responsiveness.

Besides incoming emails – there are many other benefits to CCT including the screening of downloads from web sites that are talked about in the article titled Drive-By Internet Infections later on in this newsletter.

**Microsoft – NEXTGEN**

I have been evaluating on behalf of my customers both Windows 2008 (W2008) and Small Business Server 2008 for more than half a year. My experiences have been okay – but

these are Beta systems – and its not totally fair to judge Microsoft's next generation by a beta. My main observation is that there is nothing exciting enough that I have found to make it worthwhile to migrate customers in the near future.

TODAY – May 13, 2008, Microsoft has finally announced their plans – and most importantly put pricing with the plans. So – here goes on what I see.

Microsoft is offering two 'packages' for the small business. Each package comes in two configurations – standard and premium.

### Small Business Server 2008

The less expensive package is Microsoft Small Business Server 2008. The standard version is a single box W2008 server configuration. The SBS2008 standard configuration comes with W2008, Exchange Server 2007, Windows Sharepoint Services 3.0 (company web, etc.), Server Update Service 3.0 (was only part of SBS2003 R2) and Microsoft Office Live Services. [At this point I don't have a full understanding of Office Live services – but I believe it allows you to create web content and use that for sales or training or other online activities]. While pricing is subject to change and discount – the cost for a 5 license system is \$1,089 and each additional user license is \$77. You may be able to purchase user licenses in single rather than 5-pack quantities.

Microsoft Small Business Server 2008 premium adds to the standard configuration by adding a second Windows 2008 Server license and SQL Server 2008. In essence – you get the opportunity for a second server for your SQL applications. This may/will prove valuable for my customers who rely upon SQL for a mainstay application or two. SBS2008 premium will sell for \$1,899 and additional user licenses will be \$189.

It looks like basic prices have gone up – but the additional licenses for Standard are lower. In addition, you can purchase a mixture of standard and premium licenses – depending upon how many people you have need to access the SQL server.

What isn't included is significant. There is no Remote Desktop and no ISA firewall. What Microsoft is saying – is that you will have to obtain ISA separately – if you choose that for a firewall. You will also have to find another way to do remote desktop – which for many of my customers is the 'killer' application for which they purchased SBS2003. The CCT product mentioned earlier was **SPECIFICALLY** developed knowing this was going to happen and is capable of providing both firewall and remote desktop access to your SBS2008 network.

Release of the SBS2008 product is still scheduled for the second half of 2008.

### Windows Essential Business Server 2008

Windows Essential Business Server 2008 (EBS) is the more advanced and capable version of software for small businesses. It begins to mimic a significant Information Technology configuration generally found in larger offices. The price also begins to mimic a larger organization.

EBS standard version consists of two servers. The first server has Windows 2008 Server with Microsoft System Center Essentials 2008. Microsoft System Center Essentials 2008 is a management tool for the network. The second server also includes Windows 2008 Server and Exchange 2007 and Microsoft Forefront Security for Exchange Server. In essence – Forefront is an Exchange spam and virus and phishing filter. The cost of EBS standard is \$5,472 with additional licenses costing \$87 each.

EBS premium version consists of EBS standard plus two additional servers. One additional server is another Exchange Server with the next version of ISA for the firewall and the second server is for an SQL database. This package sells for \$7163 for a 5 user license and \$197 per additional license.

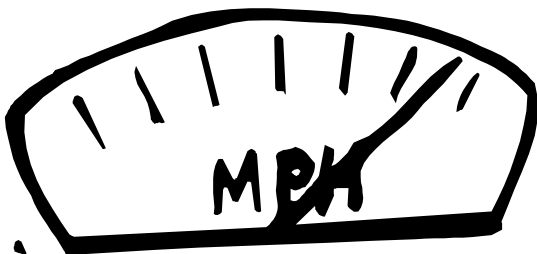
With the exception of EBS premium – there is no firewall and since the capabilities of the next generation ISA are not know – the ability to do remote desktop is also not defined.

Microsoft has once again changed their sizing recommendations. SBS2008 is recommended for up to 50 workstations while EBS is recommended for up to 250 workstations. It is not know at this time if these are enforced limits or just recommendations. One must keep in mind that these prices are significantly less than the cost of the products if purchased individually – and one would hope that the integration and management of these servers is much better than would be obtained by a looser coupled set of products.

These servers are all 64 bit – so please understand that none of the server hardware that you currently have installed will likely be of much value in a new system.

For more information on these products, Microsoft has set up a new web site at <http://MultiplyYourPower.com>. As I know more information – I will provide updates. Of course – we will continue to test and verify the claims, stability and efficiency of these new servers.

### Drive-by Internet Infections



According to Industry sources there are two major mechanisms by which malware writers are infecting computers. The one that is most easily recognized are bogus links in emails that seem too good to be true. Users have gotten smarter about not clicking on those links. The other type is called ‘drive-by’ infection and is caused by web sites to which your browser surfs.

Your ‘browser’ – and I put it in quotes for a reason - consists of more pieces than just what Microsoft supplies. It has plug-ins from adobe such as Flash and Acrobat. It has plug-ins from Apple such as QuickTime. These plug-ins also have vulnerabilities. The most widely used plug-in is JavaScript. You can disable JavaScript – but then it is really hard to surf the Internet successfully as many sites expect to be able to communicate with you using JavaScript. So – what is one supposed to do?

First – keep your software up to date. If you use JavaScript – make sure you have the latest downloaded. QuickTime is currently on version 7.4.5 which patches 11 known vulnerabilities.

In addition, the writers of the operating system and some plug-ins are trying to help. One mechanism is called Data Execution Prevention (DEP). Basically – DEP doesn’t allow an area of memory that is dedicated to data – to suddenly become code. Downloading data that is really code (unbeknownst to the user) and then starting a program in the data memory is a favorite exploited vulnerability.

Another form of prevention that is being used is Address Space Layout Randomization (ASLR). ALSR is used by programs to change the way they appear to would-be invaders. Modules and code are loaded in different orders and to different memory locations. In that way – a invasion program that expects to find a module at a known location – can’t as it’s moved.

Links to web sites that contain malicious code can be found in Google and other search engines. While these engines try to make sure

they don't link to malicious code – they have a hard time checking and rechecking every link. At one point, Google's search mechanism had as many as 40.000 links to malicious web sites.

While training humans to be good surfers sounds like a great plan, there has to be another way to combat this malicious code. One way is to have every page that is downloaded to your browser inspected for vulnerabilities. This is called stateful inspection and can be done by a 'box' remote from your browser which is checking before you browser is given the response from a web site. Armed with a list of known vulnerabilities a clever interface device such as the CCT can recognize malicious code and block it.

In my opinion, this form of drive-by infection is going to be come significantly more common and represents the current greatest threat to your happy office environment.

## **Security Issues**

Microsoft has issued 4 security updates this month. It's May and we are already at update 28. This appears to becoming another year with a projected record number of patches coming down the line.

Below is the list and a link to Microsoft's explanations. Please apply these to your workstations.

### **Critical**

- [MS08-026](#) - Vulnerabilities in Microsoft Word Could Allow Remote Code Execution
- [MS08-027](#) - Vulnerability in Microsoft Publisher Could Allow Remote Code Execution
- [MS08-028](#) - Vulnerability in Microsoft Jet Database Engine Could Allow Remote Code Execution

### **Moderate**

- [MS08-029](#) - Vulnerabilities in Microsoft Malware Protection Engine Could Allow Denial of Service