

Re: << SBS News of the week – Sept 26 >>

Source:

<http://www.tech-archive.net/Archive/BackOffice/microsoft.public.backoffice.smallbiz2000/2004-09/1455.html>

From: Cris Hanna \((SBS-MVP)\) (*crishannanospam_at_computingpossibilities.net*)

Date: 09/29/04

Date: Tue, 28 Sep 2004 21:53:48 -0500

rtf

--
CRIS HANNA
SBS-MVP

Please do not respond to me directly by email but only in the newsgroups so that all can benefit from the information
"Susan Bradley, CPA aka Ebitz - SBS Community Rocks" <sbradcpa@pacbell.net> wrote in message news:uPl8m%23EpEHA.3988@tk2msftngp13.phx.gbl...

>
> Jeanne is moving up the USA coast and Kevin still writes a song
> [news://msnews.microsoft.com/e\\$IzqfgoEHA.3464@TK2MSFTNGP14.phx.gbl](http://news://msnews.microsoft.com/e$IzqfgoEHA.3464@TK2MSFTNGP14.phx.gbl)

> -----
>
> Harry Brelsford's September 2004 SMB Technology Watch Newsletter:
> <http://www.smbnation.com/newsletter/Issue4-3-September2004.htm>

> -----
>
> We have a new fix to allow workstations to roll out SP2 automagically
> <http://msmvps.com/cgross/archive/2004/09/24/14251.aspx>
> Chad points to the new update that allows workstations to get sp2 rather
> than sp1 when they /connectcomputer to the server
> And he points to the info you need to put the file on the server in the
> right place:
> Preparing XP SP2 for deployment on SBS 2003:
> <http://msmvps.com/cgross/archive/2004/09/26/14393.aspx>

> -----
>
> Introducing the Microsoft Exchange Best Practices Analyzer Tool:
> <http://blogs.msdn.com/exchange/archive/2004/09/21/232516.aspx>

>
> Hi folks,

>
> We just released an update to the rules. If you have Internet
> connectivity from your workstation, then the tool should auto-detect the
> update and prompt you to download. If you're working in a closed
> environment, or the tool doesn't manage to detect the update, then you
> can download and apply the "Web Update Pack" from

> <http://www.microsoft.com/downloads/details.aspx?FamilyID=4f2f1339-cbcd-4d26-9174-f30c10d7ec4c>.

> Simply extract the files to your installation folder (usually,
> C:\Program Files\ExBPA). Within a short period of time we'll also have a
> link to the Web Update Pack from our main

>
> <http://www.microsoft.com/exchange/exbpa>"><http://www.microsoft.com/exchange/exbpa>

microsoft.public.backoffice.smallbiz2000: Re: << SBS News of the week – Sept 26 >>

> page.

>

> If you want to double-check if the update is applied, then click the
> "About..." link in the left-hand navigator when the tool is open. You'll
> see two version numbers ...the first is 1.0.7408.1 ...this is the
> version of the main binaries. The second version number is what we call
> the "ConfigVersion". You'll see one of the following:

>

> 1.5.4.0 = You're running the rules as shipped in the original MSI package
> 1.5.5.1 = You're running the rules update that we posted a few days ago
> 1.5.6.1 = You're running the very latest rules available

>

> These latest rules include some refinements that we made in response to
> the postings on the newsgroup and the blogs that we're monitoring.

>

> Please keep the feedback coming! Through your help we can further refine
> the rules and documentation so that you see only the issues which are
> relevant for you.

>

> --

> Paul Bowden
> Program Manager
> Exchange Server Best Practices Analyzer
> <http://www.microsoft.com/exchange/exbpa>

>

> -----

>

> Speaking of blogs...

>

> If you've found a really good SBS blog or SBS related blog
> Please forward the link

>

> I've just started to list them on www.sbslinks.com

>

> -----

> KB's of interest
> 875422 - "The wizard cannot set the DHCP scope options" error message
> when you run the Configure E-mail and Internet Connection Wizard in
> Windows Small Business Server 2003:

> <http://support.microsoft.com/?kbid=875422>

> 873434 - The Exchange Intelligent Message Filter does not scan e-mail
> messages on your Exchange Server 2003 computer:

> <http://support.microsoft.com/?kbid=873434>

>

> An email from Scott Schnell:

> <http://msmvps.com/bradley/archive/2004/09/23/14182.aspx>

>

> Did everyone check this out?

>

> This is so off topic it's not funny but ... hey
> Amazon.com: DVD: Star Wars Trilogy (Widescreen Edition):

>

> http://www.amazon.com/exec/obidos/tq/detail/-/B00003CXCT/qid=1096259172/sr=8-1/ref=pd_csp_1/102-0

>

> The Star Wars DVD is out

> Star Wars: Episode IV | Star Wars Trilogy on DVD:

> http://www.starwars.com/episode-iv/trilogy_dvd.html

> Star Wars: Community | Wallpaper:

> <http://www.starwars.com/community/downloads/wallpaper/>

>

> -----

>

Re: << SBS News of the week – Sept 26 >>

microsoft.public.backoffice.smallbiz2000: Re: << SBS News of the week – Sept 26 >>

> Are you patching for GPIplus?
> UPDATE: Microsoft JPEG Image Processing Overflow (MS04-028)
>
> Description: Multiple exploits and a toolkit (posted on the th-research
> mailing list) that create specially crafted JPEG files are now
> available. Viewing such JPEG files using Internet Explorer, Outlook,
> Word etc., results in the execution of arbitrary code. Some security
> analysts predict the outbreak of an email virus exploiting the JPEG
> vulnerability by the end of this month.
>
> Council Site Actions: All of the council sites have either patched the
> systems, are in the process of patching the systems (or testing the
> patches) or plan to patch in the near future. In addition, one site is
> working with their network staff to enable appropriate IPS-like filters
> at the network perimeter. Another site reported they were hit with this
> attack and have taken steps to block it (details not provided).
>
> References:
> Various Exploits
> <http://www.securiteam.com/exploits/5EP0M0KE0W.html>
> (Opens a command shell)
> <http://archives.neohapsis.com/archives/fulldisclosure/2004-09/0819.html>
> (Adds an administrator)
> <http://www.securityfocus.com/archive/1/376320/2004-09-23/2004-09-29/0>
> (Binds a remote command shell or opens a reverse command shell)
> SANS GDI Detection Tool
> <http://isc.sans.org/qdiscan.php>
> Previous @RISK Newsletter Posting
> http://www.sans.org/newsletters/risk/vol3_37.php (Item #1)
> 3) CRITICAL: Symantec Firewall/VPN Default SNMP Community String
> Affected:
> Symantec Firewall/VPN Appliance 100, 200/200R (firmware builds prior to
> build 1.63)
> Symantec Gateway Security 320, 360/360R (firmware builds prior to build
> 622)
>
> Macromedia is not affected
> http://www.macromedia.com/devnet/security/security_zone/mpsb04-07.html
>
> -----
> Description: The Symantec Firewall/VPN and the Gateway Security
> appliances are designed to protect small business networks. These
> appliances use "public" as the default read/write community string for
> the SNMP service. In addition, the appliances do not perform sufficient
> checks on the UDP packets with the source port set to 53 i.e. a DNS
> response. An attacker can exploit these flaws in tandem via specially
> crafted SNMP "GET" or "SET" requests with a source port of 53. Such
> crafted requests may permit the attacker to make arbitrary changes to
> the firewall configuration, thereby putting the entire network protected
> by the firewall at risk. Note that the firewall administrator can
> neither disable the SNMP service nor change the default SNMP community
> string.
>
> Status: Symantec confirmed. Firmware updates are available for all the
> affected products. The updates also fix a denial of service attack
> vulnerability that can be triggered by performing a UDP scan on the
> firewall appliances.
>
> Council Site Actions: The affected software is not in production or
> widespread use at any of the council sites. They reported that no action
> was necessary.
>

Re: << SBS News of the week – Sept 26 >>

> References:

> Posting by Mike Sues

> <http://www.securityfocus.com/archive/1/376029/2004-09-20/2004-09-26/0>

> Symantec Advisory

> <http://www.sarc.com/avcenter/security/Content/2004.09.22.html>

> Product Homepage

> <http://www.symantec.com/smallbiz/qtw/>

> SecurityFocus BID

> <http://www.securityfocus.com/bid/11237>

>

>

>

> *****

>

> HIGH: Alt-N MDAemon Multiple Buffer Overflows

> Affected: MDAemon version 6.5.1

>

> Description: The MDAemon SMTP and IMAP server contain multiple buffer
> overflows. The flaws in the SMTP server can be triggered by sending
> overlong arguments to the "SAML", "SOML", "SEND" or "MAIL" commands, and
> the flaw in the IMAP server can be triggered by an overlong argument to
> the "LIST" command. The flaws may be possibly exploited to execute
> arbitrary code with "SYSTEM" privileges on the Windows server running
> the MDAemon software. Whereas an attacker needs authentication
> privileges to exploit the flaw in the IMAP server, depending on the
> configuration, the flaws in the SMTP server may be exploited by an
> unauthenticated attacker. The proof-of-concept exploit code has been
> publicly posted.

>

> Status: Vendor not confirmed, no updates available.

>

> Council Site Actions: The affected software is not in production or
> widespread use at any of the council sites. They reported that no action
> was necessary.

>

> References:

> Posting by pigrelax

> <http://www.securityfocus.com/archive/1/376082/2004-09-20/2004-09-26/0>

> Proof-of-concept Exploit Code

> <http://www.securitylab.ru/48146.html>

> http://www.securitylab.ru/Exploits/2004/09/mdaemon_rcpt.c

> http://www.securitylab.ru/Exploits/2004/09/mdaemon_imap.c

> Product Homepage

> <http://www.altn.com/products/default.asp?product%5Fid=MDaemon>

> SecurityFocus BID

> <http://www.securityfocus.com/bid/11238>

>

> -----

> In other news

> A man admits hacking into computers of high tech company
> According to the Plea Agreement, Mr. Erfurt admitted
> that, on January 23 and 24, 2003, he hacked into the
> computer system of MESC by using a computer from his
> workplace at a separate company in Irvine, California.
> Mr. Erfurt had previously served as the Information
> Technology Manager and then as Network Manager for
> MESC. After gaining unauthorized access to MESC's
> computer system, Mr. Erfurt admitted that he
> downloaded a proprietary database, read the e-mail
> account of the company president, and deleted
> data from the servers.
> <http://www.crime-research.org/news/24.09.2004/646/>

> - - - - -

> Four Los Alamos lab workers fired over security, safety lapses
> Four laboratory workers were fired from their
> jobs at the Los Alamos National Laboratory because
> of their roles in several recent security and safety
> incidents in the facility. One other worker resigned
> in lieu of being fired, while seven other workers
> faced disciplinary actions, including demotions,
> pay cuts and suspensions or reprimands, according
> to Kevin Roark, a spokesman for the New Mexico-
> based facility. Another 10 workers who were under
> investigation in connection with the problems have
> returned to their jobs after being cleared of
> wrongdoing, according to Roark. One employee
> remains on paid leave.

>

> <http://computerworld.com/securitytopics/security/story/0,10801,96169,00.html>

> - - - - -

> Hackers use Google to access photocopiers
> Making copies of something important? Photocopiers
> are the latest networked devices to fall prey
> to hackers armed with nothing more than Google's
> search engine. Hackers are using search engines
> to watch what people photocopy. Using Google hacks
> -- requests typed into the search engine that bring
> up cached information on networks -- hackers are
> discovering and using login details for networked
> photocopiers so they can watch what is being copied.
> <http://news.zdnet.co.uk/internet/security/0,39020375,39167848,00.htm>

> - - - - -

> FDIC warns consumers on e-mail scams
> Banking agency warns of 'phish' schemes. The FDIC
> Friday issued an alert about an increasingly common
> e-mail scam designed to steal personal information
> and money from millions of unwary consumers. The
> Federal Deposit Insurance Corp. (FDIC), perhaps
> best known as an insurer of bank deposits, issued
> its warning about so-called "phishing" eight months
> after criminals began misappropriating its name
> and reputation to perpetrate e-mail fraud.
> <http://msnbc.msn.com/id/6091951/>

>

> Invasion of the identity snatchers
> http://www.theregister.co.uk/2004/09/24/identity_snatchers/
> Credit card leaks continue at furious pace
> <http://msnbc.msn.com/id/6030057/>

> - - - - -

> Speedy cybersecurity legislation killed by turbulence
> An attempt by House Republican leaders to
> strengthen the Office of Management and Budget's
> role in cybersecurity was withdrawn late Thursday
> after industry and government officials voiced
> their opposition to the provision in legislation
> overhauling the U.S. intelligence community. Media
> reports this week had described the legislation
> as shifting responsibility for cybersecurity from
> the Homeland Security Department to the Office of
> Management and Budget. But David Marin, spokesman
> for Rep. Tom Davis (R-Va.), chairman of the House
> Government Reform Committee, disputed that.
> http://www.gcn.com/voll_nol/daily-updates/27449-1.html

> - - - - -

microsoft.public.backoffice.smallbiz2000: Re: << SBS News of the week – Sept 26 >>

> Piracy cut back by compliance laws
> Having to fit in with new laws is keeping big businesses
> in line when it comes to counterfeit software - but their
> smaller counterparts are still a problem. New compliance
> and accounting regulations are helping to drive down the
> number of firms who use unlicensed and counterfeit
> software, according to Microsoft.
> <http://news.zdnet.co.uk/business/legal/0,39020651,39167738,00.htm>
> - - - - -
> Virus writers hit home PCs as companies get tough
> Stronger corporate defences make poorly protected
> home users easier targets. Virus writers are
> increasingly targeting poorly protected home
> PCs because company defences are proving too much
> of a challenge. Vincent Gullotto, vice president
> of the Anti-Virus Emergency Response Team (Avert)
> at security company McAfee, said recent attacks
> have ignored corporate networks and aimed for
> the home user instead.
> <http://www.vnunet.com/news/1158338>
>
> JPEG File Flaw Prompts New Wave of Attacks
>
http://www.newsfactor.com/story.xhtml?story_title=JPEG-File-Flaw-Prompts-New-Wave-of-Attacks&stor
> - - - - -
> MS fires armour-piercing suit at 'bullet-proof' spam host
> Microsoft has fired off nine new lawsuits against
> spammers including an action against a web
> hosting firm that allegedly offered so-called
> "bullet proof" hosting to junk mailers. National
> Online Sales and its owner Levon Gillespie are
> jointly accused of offering a "safe haven" for
> purveyors of get-rich-quick schemes and penis
> enlargement rackets. The case was filed in
> Washington State's King County Superior Court.
> http://www.theregister.co.uk/2004/09/24/ms_anti-spam_lawsuit/
> <http://money.cnn.com/2004/09/23/technology/msftspam.reut/index.htm>
>
> Sender ID dealt killer blow
> <http://news.zdnet.co.uk/software/applications/0,39020384,39167720,00.htm>
> - - - - -
> Symantec Warns of Firewall Weakness
> Symantec says it has identified security flaws in
> several of its firewall and gateway products that
> could leave networks vulnerable to denial-of-service
> attacks. The security company has issued firmware
> upgrades to close the loopholes.
>
http://www.newsfactor.com/story.xhtml?story_title=Symantec-Warns-of-Firewall-Weakness&story_id=27
> - - - - -
> When they start making Sponge Bob Square Pants Secure ID tokens... we're
> in trouble :-)
>
> VeriSign creates kid credentials
> VeriSign and a children's safety group has unveiled
> a new technology designed to make it easier for
> children to avoid child predators online. The i-Stik
> token, inserted in a computer's USB port, provides
> verification of a child's age and gender. Chatroom
> lurkers who can't prove their age will stick out
> like sore thumbs as more kids adopt the tokens,
> backers said.

Re: << SBS News of the week – Sept 26 >>

microsoft.public.backoffice.smallbiz2000: Re: << SBS News of the week – Sept 26 >>

> http://news.zdnet.com/2100-1009_22-5380589.html
> - - - - -
> So what is it about Win2k security MS won't enhance?
> If you want the 'security enhancements' of Windows XP
> SP2 but you're running an earlier version of Windows,
> then you're going to have to upgrade, Microsoft has
> been confirming to the public prints this week. Despite
> this being highly significant for the many companies
> still running Windows 2000, Microsoft has been
> confirming it pretty quietly - CNET and Microsoft
> Watch both seem to have been given statements on
> demand, and Redmond does not yet seem to be exactly
> bulging with detail on the subject.
> http://www.theregister.co.uk/2004/09/24/no_sp2_fixes_for_old_windows/
>
>
>
>
>
>
> --
> <http://www.sbslinks.com/really.htm>
> <http://www.msmvps.com/bradley>
> <https://www.ecora.com/ecora/jump/pm99.asp>

Re: << SBS News of the week – Sept 26 >>