

microsoft.public.windows.server.sbs: Re: <<< Small Biz Server this week July 18th 2004 >>>

Re: <<< Small Biz Server this week July 18th 2004 >>>

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2004-07/4757.html>

From: Henry Craven (*IUnknown_at_Dot.Nyet*)

Date: 07/19/04

Date: Tue, 20 Jul 2004 02:22:06 +1000

rtf

--

Henry Craven {SBS-MVP}

Melbourne Australia

"Susan Bradley, CPA aka Ebitz - SBS Rocks [MVP]" <sbradcpa@pacbell.net>
wrote in message news:uRqgMcVbEHA.3148@TK2MSFTNGP10.phx.gbl...

> NEWSGROUP POSTS OF INTEREST

>

> Song of the week

> <news://msnews.microsoft.com/#5LKc65aEHA.3892@TK2MSFTNGP10.phx.gbl>

>

> And Jeff's funny post about redundant MVPs ;-)

> <news://msnews.microsoft.com/#kb3BBeaEHA.1840@TK2MSFTNGP11.phx.gbl>

>

> Moving to new hardware?

> Check this out....

> <news://msnews.microsoft.com/uNqskk0aEHA.2388@TK2MSFTNGP11.phx.gbl>

>

> Proposed Posting FAQs

> <news://msnews.microsoft.com/ehuS7J6aEHA.2840@TK2MSFTNGP11.phx.gbl>

>

> -----

>

> ONLINE EVENTS

> SBS Live Chat

> <http://www.mcpmag.com/chats/>

> Tuesday

> 7/20/04 - 4:00 PM

> (16:00 PST) #MCPmag SBS Live! Andy Goodman

>

> -----

> IN THE NEWS

> Small Biz in the news

> ITBusiness.ca:

>

> <http://www.itbusiness.ca/index.asp?theaction=61&lid=1&sid=56153&adBanner=Security>

>

> Trend Micro to Provide Virus and Spam Protection for HP ProLiant Servers

> for Small Businesses

> <http://www.cnw.ca/fr/releases/archive/July2004/12/c2279.html>

>

Re: <<< Small Biz Server this week July 18th 2004 >>>

microsoft.public.windows.server.sbs: Re: <<< Small Biz Server this week July 18th 2004 >>>

> If you sell, install SBS and you haven't signed up as a registered
> partner... why NOT?
> Microsoft gets specific with partner program - News - ZDNet:
> http://zdnet.com.com/2100-1104_2-5266552.html
>
> -----
> SECURITY PATCHES THIS WEEK
>
> Security patches this week...
>
> And just to let you know that while worms are not "live on the web",
> exploit code is circulating
>
> <http://www.incidents.org/diary.php?date=2004-07-18&isc=ed26c333a2f2f59997f9ed707d0ed6d1>
>
> Today 13 July 2004, Microsoft is releasing 7 security updates for
newly
> discovered vulnerabilities in Microsoft Windows.
>
> - One Microsoft Security Bulletin affecting Microsoft Windows with a
> maximum severity of Moderate, MS04-018
> - One Microsoft Security Bulletin affecting Microsoft Windows with a
> maximum severity of Important, MS04-019
> - One Microsoft Security Bulletin affecting Microsoft Windows with a
> maximum severity of Important, MS04-020
> - One Microsoft Security Bulletin affecting Microsoft Windows with a
> maximum severity of Important, MS04-021
> - One Microsoft Security Bulletin affecting Microsoft Windows with a
> maximum severity of Critical, MS04-022
> - One Microsoft Security Bulletin affecting Microsoft Windows with a
> maximum severity of Critical, MS04-023
> - One Microsoft Security Bulletin affecting Microsoft Windows with a
> maximum severity of Important, MS04-024
> Per Incidents.org web site, they are kicking up the Criticality of
> 04-024 [the shell patch] because of "public availability of the
> exploit"
>
>
> Summaries for these new bulletins may be found at the following page:
> - <http://www.microsoft.com/technet/security/bulletin/ms04-jul.mspx>
>
> Customers are advised to review the information in the bulletins, test
> and deploy the updates immediately in their environments, if
applicable.
>
> Microsoft will host a webcast tomorrow to address customer questions
on
> these bulletins. For more information on this webcast please see
below:
> - Information about Microsoft's July Security Bulletins
> - Wednesday, July 14, 2004 10:00 AM - Wednesday, July 14, 2004 11:00
AM
> (GMT-08:00) Pacific Time (US & Canada)
> - <http://go.microsoft.com/fwlink/?LinkId=30865>
>
> - The on-demand version of the webcast will be available 24 hours
after
> the live webcast at:
> - <http://go.microsoft.com/fwlink/?LinkId=30865>
>
> MS04-018
>

Re: <<< Small Biz Server this week July 18th 2004 >>>

microsoft.public.windows.server.sbs: Re: <<< Small Biz Server this week July 18th 2004 >>>

> Title: Cumulative Security Update for Outlook Express (823353)
>
> Affected Software:
> - Microsoft Windows NT Workstation 4.0 Service Pack 6a
> - Microsoft Windows NT Server 4.0 Service Pack 6a
> - Microsoft Windows NT Server 4.0 Terminal Server Edition Service
Pack 6
> - Microsoft Windows 2000 Service Pack 2, Microsoft Windows 2000
Service
> Pack 3, Microsoft Windows 2000 Service Pack 4
> - Microsoft Windows XP and Microsoft Windows XP Service Pack 1
> - Microsoft Windows XP 64-Bit Edition Service Pack 1
> - Microsoft Windows XP 64-Bit Edition Version 2003
> - Microsoft Windows Server 2003
> - Microsoft Windows Server 2003 64-Bit Edition
> - Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE),
and
> Microsoft Windows Millennium Edition (Me) - Review the FAQ section of
> this bulletin for details about these operating systems.
>
> Affected Components:
> - Microsoft Outlook Express 5.5 Service Pack 2
> - Microsoft Outlook Express 6
> - Microsoft Outlook Express 6 Service Pack 1
> - Microsoft Outlook Express 6 Service Pack 1 (64 bit Edition)
> - Microsoft Outlook Express 6 on Windows Server 2003
> - Microsoft Outlook Express 6 on Windows Server 2003 (64 bit
edition)
>
> Impact of Vulnerability: Denial of Service
>
> Maximum Severity Rating: Moderate
>
> Restart required: In some cases, this update does not require a
> restart. The installer stops the required services, applies the
update,
> and then restarts the services. However, if the required services
cannot
> be stopped for any reason or if required files are in use, this update
> will require a restart. If this occurs, a message appears that advises
> you to restart.
>
> Update can be uninstalled: Yes
>
> More information on this vulnerability is available at:
> <http://www.microsoft.com/technet/security/bulletin/MS04-018.mspx>
> *****
>
> MS04-019
>
> Title: Vulnerability in Utility Manager Could Allow Code Execution
> (842526)
>
> Affected Software:
> - Microsoft Windows 2000 Service Pack 2, Microsoft Windows 2000
Service
> Pack 3, Microsoft Windows 2000 Service Pack 4
>
> Impact of Vulnerability: Local Elevation of Privilege
>
> Maximum Severity Rating: Important
>

Re: <<< Small Biz Server this week July 18th 2004 >>>

microsoft.public.windows.server.sbs: Re: <<< Small Biz Server this week July 18th 2004 >>>

> Restart required: In some cases, this update does not require a
> restart. The installer stops the required services, applies the
update,
> and then restarts the services. However, if the required services
cannot
> be stopped for any reason or if required files are in use, this update
> will require a restart. If this occurs, a message appears that advises
> you to restart.
>
> Update can be uninstalled: Yes
>
> More information on this vulnerability is available at:
> <http://www.microsoft.com/technet/security/bulletin/MS04-019.msp>
> *****
>
> MS04-020
>
> Title: Vulnerability in POSIX Could Allow Code Execution (841872)
>
> Affected Software:
> - Microsoft Windows NT Workstation 4.0 Service Pack 6a
> - Microsoft Windows NT Server 4.0 Service Pack 6a
> - Microsoft Windows NT Server 4.0 Terminal Server Edition Service
Pack
> 6
> - Microsoft Windows 2000 Service Pack 2, Microsoft Windows 2000
Service
> Pack 3, Microsoft Windows 2000 Service Pack 4
>
> Impact of Vulnerability: Local Elevation of Privilege
>
> Maximum Severity Rating: Important
>
> Restart required: In some cases, this update does not require a
restart.
> The installer stops the required services, applies the update, and
then
> restarts the services. However, if the required services cannot be
> stopped for any reason or if required files are in use, this update
will
> require a restart. If this occurs, a message appears that advises you
to
> restart.
>
> Update can be uninstalled: Yes
>
> More information on this vulnerability is available at:
> <http://www.microsoft.com/technet/security/bulletin/MS04-020.msp>
> *****
>
> MS04-021
>
> Title: Security Update for IIS 4.0 (841373)
>
> Affected Software:
> - Microsoft Windows NT Workstation 4.0 Service Pack 6a
> - Microsoft Windows NT Server 4.0 Service Pack 6a
>
> Affected Components:
> - Microsoft Internet Information Server (IIS) 4.0
>
> Impact of Vulnerability: Remote Code Execution

Re: <<< Small Biz Server this week July 18th 2004 >>>

microsoft.public.windows.server.sbs: Re: <<< Small Biz Server this week July 18th 2004 >>>

>
> Maximum Severity Rating: Important
>
> Restart required: Yes
>
> Update can be uninstalled: Yes
>
> More information on this vulnerability is available at:
> <http://www.microsoft.com/technet/security/bulletin/MS04-021.mspx>
> *****
>
> MS04-022
>
> Title: Vulnerability in Task Scheduler Could Allow Code Execution
> (841873)
>
> Affected Software:
> - Microsoft Windows 2000 Service Pack 2, Microsoft Windows 2000
Service
> Pack 3, Microsoft Windows 2000 Service Pack 4
> - Microsoft Windows XP and Microsoft Windows XP Service Pack 1
> - Microsoft Windows XP 64-Bit Edition Service Pack 1
>
> Affected Components:
> - Internet Explorer 6 when installed on Windows NT 4.0 SP6a
> (Workstation, Server, or Terminal Server Edition)
>
> Impact of Vulnerability: Remote Code Execution
>
> Maximum Severity Rating: Critical
>
> Restart required: In some cases, this update does not require a
restart.
> The installer stops the required services, applies the update, and
then
> restarts the services. However, if the required services cannot be
> stopped for any reason or if required files are in use, this update
will
> require a restart. If this occurs, a message appears that advises you
to
> restart.
>
> Update can be uninstalled: Yes
>
> More information on this vulnerability is available at:
> <http://www.microsoft.com/technet/security/bulletin/MS04-022.mspx>
> *****
>
> MS04-023
>
> Title: Vulnerability in HTML Help Could Allow Code Execution (840315)
>
> Affected Software:
> - Microsoft Windows 2000 Service Pack 2, Microsoft Windows 2000
Service
> Pack 3, Microsoft Windows 2000 Service Pack 4
> - Microsoft Windows XP and Microsoft Windows XP Service Pack 1
> - Microsoft Windows XP 64-Bit Edition Service Pack 1
> - Microsoft Windows XP 64-Bit Edition Version 2003
> - Microsoft Windows Server 2003
> - Microsoft Windows Server 2003 64-Bit Edition
> - Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE),

Re: <<< Small Biz Server this week July 18th 2004 >>>

microsoft.public.windows.server.sbs: Re: <<< Small Biz Server this week July 18th 2004 >>>

and

> Microsoft Windows Millennium Edition (ME) - Review the FAQ section of
> this bulletin for details about these operating systems.
>
> Affected Components:
> - Internet Explorer 6.0 Service Pack 1 when installed on Windows NT
4.0
> SP6a (Workstation, Server, or Terminal Server Edition)
>
> Impact of Vulnerability: Remote Code Execution
>
> Maximum Severity Rating: Critical
>
> Restart required: In some cases, this update does not require a
restart.
> The installer stops the required services, applies the update, and
then
> restarts the services. However, if the required services cannot be
> stopped for any reason or if required files are in use, this update
will
> require a restart. If this occurs, a message appears that advises you
to
> restart.
>
> Update can be uninstalled: Yes
>
> More information on this vulnerability is available at:
> <http://www.microsoft.com/technet/security/bulletin/MS04-023.msp>
> *****
>
> MS04-024
>
> Title: Vulnerability in Windows Shell Could Allow Remote Code
Execution
> (839645)
>
> Affected Software:
> - Microsoft Windows NT(r) Workstation 4.0 Service Pack 6a
> - Microsoft Windows NT Server 4.0 Service Pack 6a
> - Microsoft Windows NT Server 4.0 Terminal Server Edition Service
Pack
> 6
> - Microsoft Windows NT(r) Workstation 4.0 Service Pack 6a with
Active
> Desktop
> - Microsoft Windows NT Server 4.0 Service Pack 6a with Active
Desktop
> - Microsoft Windows NT Server 4.0 Terminal Server Edition Service
Pack
> 6 with Active Desktop
> - Microsoft Windows 2000 Service Pack 2, Microsoft Windows 2000
Service
> Pack 3, Microsoft Windows 2000 Service Pack 4
> - Microsoft Windows XP and Microsoft Windows XP Service Pack 1
> - Microsoft Windows XP 64-Bit Edition Service Pack 1
> - Microsoft Windows XP 64-Bit Edition Version 2003
> - Microsoft Windows Server 2003
> - Microsoft Windows Server 2003 64-Bit Edition
> - Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE),
and
> Microsoft Windows Millennium Edition (ME) - Review the FAQ section of
> this bulletin for details about these operating systems.

Re: <<< Small Biz Server this week July 18th 2004 >>>

microsoft.public.windows.server.sbs: Re: <<< Small Biz Server this week July 18th 2004 >>>

>
> Impact of Vulnerability: Remote Code Execution
>
> Maximum Severity Rating: Important
>
> Restart required: In some cases, this update does not require a
> restart. The installer stops the required services, applies the
update,
> and then restarts the services. However, if the required services
cannot
> be stopped for any reason or if required files are in use, this update
> will require a restart. If this occurs, a message appears that advises
> you to restart.
>
> Update can be uninstalled: Yes
>
> More information on this vulnerability is available at:
> <http://www.microsoft.com/technet/security/bulletin/MS04-024.msp>
> *****
>
> PLEASE VISIT <http://www.microsoft.com/technet/security> FOR THE MOST
> CURRENT INFORMATION ON THESE ALERTS.
> -----
>
> IN OTHER NEWS ...
>
> Martha Stewart gets 5 months....
> New York Times hacker Adrian Lamo gets home detention
> He was also sentenced to two years' probation and fined
> more than \$64,900. Adrian Lamo, who gained a reputation
> as the "homeless hacker" for his itinerant lifestyle,
> will be considerably easier to find -- at least for
> the next few months. Lamo was sentenced yesterday to
> six months of home confinement after pleading guilty
> in January to charges that he broke into the internal
> computer network of The New York Times Co.
>
<http://computerworld.com/securitytopics/security/story/0,10801,94600,00.html>
> - - - - -
> Feds ask state to check computer servers
> The appearance in a state computer of files containing
> texts and images that apparently originated with the
> terrorist group al-Qaeda prompted the federal Homeland
> Security Department to wonder about the security of
> other state computers. Gary Underwood, chief security
> officer for the state computer network, said that after
> a check this week of the state's computer system's
> servers, it seems the terrorist-related files were
> an isolated incident.
>
http://www.usatoday.com/tech/news/computersecurity/2004-07-16-arkansas-servers_x.htm
> - - - - -
> Judge fines spammer \$4m
> A federal judge in California has awarded Microsoft
> \$4m (£2.13bn) after finding that a California man
> and his company had sent spam, or unsolicited email,
> to users of its MSN and Hotmail services to get them
> to download a toolbar onto their computer desktops.
> Judge Manuel Real of the US Central District Court
> of California found that Daniel Khoshnood and Pointcom
> had violated several laws against using deceptive
> email and web addresses, ordering the defendants

Re: <<< Small Biz Server this week July 18th 2004 >>>

microsoft.public.windows.server.sbs: Re: <<< Small Biz Server this week July 18th 2004 >>>

> to pay damages, attorneys fees and cease any activity
> that purports to be official communication from
> Microsoft.
> <http://news.zdnet.co.uk/business/legal/0,39020651,39160838,00.htm>
> http://www.theregister.co.uk/2004/07/16/ms_spam_case_win/
> - - - - -
> Source code shop shut down
> The online shop where hackers were offering Enterasys
> and Napster source code for sale has closed its doors.
> The site, which called itself the Source Code Club,
> opened on Monday but shut up virtual shop late on
> Wednesday because of its customers' fears. It also
> said it would reopen in the "near future" when it
> had found the right business model. A statement on
> the site read: "We regret to inform that SCC has
> temporarily suspended operations. Our business model
> is currently being re-designed to alleviate some
> of the initial fears our customers faced."
> http://zdnet.com.com/2100-1105_2-5272515.html
> - - - - -
> GAO reports laundry list of DHS shortcomings
> The Homeland Security Department's failure to
> implement a long list of recommendations for
> improving its operations and management has left
> security vulnerabilities in the nation's borders
> and infrastructure, the Government Accountability
> Office said. The troubled Computer Assisted
> Passenger Prescreening System II was the target
> of seven recommendations concerning the system's
> development, oversight and IT security.
> http://www.gcn.com/voll_nol/daily-updates/26636-1.html
> - - - - -
> Olympics on guard against hackers, worms and Trojan horses
> Everyone is on the lookout for Olympic infiltrators.
> Greek police get no vacation this August. The military
> has warships and anti-terrorist commandos primed. NATO
> will offer surveillance planes. Washington has sent
> over radiation scanners. Another security front line
> is quietly watched over by a French executive armed
> with only a clipboard and flow charts. His foes include
> distant hackers, invisible computer viruses, code-
> burrowing worms and the Trojan horses of the cyber age.
>
> <http://www.siliconvalley.com/mld/siliconvalley/news/editorial/9172029.htm>
> - - - - -
> Russian piracy inflicts \$1 billion damage
> As it is well-known, a problem of intellectual
> property rights protection is the sticking point
> between Russia and the US. This pointed question
> was discussed in the frames of Russia entrance
> to the WTO. However, US Assistant Secretary of
> Commerce William Lash, made sure himself of the
> efficiency of Russian law enforcement actions
> in this sphere. In answer to assurance of Russian
> Ministry of Economic Development and Trade Deputy
> Minister Andrey Sharonov and head of the Federal
> Service for Intellectual Property, Patents and
> Trademarks Boris Simonov that Russian authorities
> go the extra mile to fight fake production,
> the US official demonstrated some purchases.
> <http://www.crime-research.org/news/16.07.2004/495/>
> - - - - -

Re: <<< Small Biz Server this week July 18th 2004 >>>

microsoft.public.windows.server.sbs: Re: <<< Small Biz Server this week July 18th 2004 >>>

> Problems of Combating Computer Crimes and Cyber Terrorism
> New opportunities offered by the Internet transformed
> many legal forms of activity and through cutting down
> terms, simplified procedures of arranging deals and
> reduced distance between contracting parties, while
> increasing attendant costs.
> <http://www.crime-research.org/news/16.07.2004/494/>
> - - - - -
> - - - - -
> Worried firms consider email boycott
> Six out of 10 companies claim they will give
> up email if the threat posed by viruses, spam
> and other unwanted content is not contained
> and a viable alternative emerges. Responding
> to an email security survey carried out by
> MessageLabs a further 40 per cent said they
> feel 'worried' by the current email security
> threat to their business, with only 29 per
> cent feeling 'optimistic'.
> <http://www.vnunet.com/news/1156684>
> - - - - -
> Metasploit Framework (Part Two)
> In the first part of this article series, we
> discussed how development of an exploit is still
> a painful and time-consuming process. We discussed
> the common hindrances faced during the development
> of exploits and how the Metasploit Framework acts
> as the singular solution to these problems. After
> getting a hands-on with the concepts of exploitation
> and exploit framework we now move further and shed
> light on the internals of the Metasploit Framework.
> <http://www.securityfocus.com/infocus/1790>
> - - - - -
> Find 'Missing' clues on Web sites, e-mail
> Cryptic clues given online and on the CD-ROM will
> help players solve the mystery that develops in
> "Missing: Since January." "Missing: Since January"
> is a fresh adventure that uses the Internet and
> e-mail to make some of its game play more realistic
> and intriguing.
> <http://www.cnn.com/2004/TECH/fun.games/07/16/review.missing/index.html>
> - - - - -
> UK companies in 'blissful ignorance' over spyware threat
> Survey: Fewer than one in seven UK companies
> recognise that malicious emails could expose
> their networks to a corporate spy, say MessageLabs
> UK companies are finally wising up to the importance
> of deploying software patches and keeping their
> antivirus signatures up to date, but the increasing
> threats from Trojans and spyware have still not
> sunk in, according to a survey conducted by email
> security services firm MessageLabs.
> <http://news.zdnet.co.uk/0,39020330,39160552,00.htm>
> - - - - -
> 'Important' Windows flaw could turn critical
> Security experts are bracing themselves for a spate
> of new worms and viruses designed to exploit of the
> seven new vulnerabilities announced by Microsoft on
> Tuesday as part of its monthly patch cycle. Of the
> new vulnerabilities, Windows Shell (MS04-024)--has
> been picked out by security experts as a potential
> target for future worms and viruses.

Re: <<< Small Biz Server this week July 18th 2004 >>>

microsoft.public.windows.server.sbs: Re: <<< Small Biz Server this week July 18th 2004 >>>

> <http://zdnet.com.com/2100-1105-5268989.html>
> <http://www.vnunet.com/news/1156635>
> http://www.theregister.co.uk/2004/07/14/ms_july_patches/
>
> Microsoft delays some security updates
>
> <http://computerworld.com/securitytopics/security/story/0,10801,94532,00.html>
> Software fuse shorts bugs
>
> http://www.trnmaq.com/Stories/2004/063004/Software_fuse_shorts_bugs_063004.html
>
> --
> <http://www.sbslinks.com/really.htm>

Re: <<< Small Biz Server this week July 18th 2004 >>>