

IT@Diocesan House #11

INTERESTING WEBSITES:

This week's focus is on the Millennium Development Goals and the websites listed in Trinity Wall Street's magazine:

www.kiva.org for microfinancing

www.justfood.org for finding a Community Supported Agriculture organization

www.er-d.org for coffee that's fair trade

www.traidcraftshop.co.uk for other fair trade goods (British so shipping can be a challenge)

www.terrapass.org for buying carbon credits to offset vacation and air travel

FREE Apple Training:

Bethlehem:

Thursday, Jul 26, 2007: 06:30 PM-07:30 PM, at Double Click

[POS and Inventory Management](#)

POS and Inventory Management

IT IN the NEWS:

From the Wall Street Journal (courtesy of Bishop Paul Marshall):

Microsoft to Alter Windows Vista

http://www.nytimes.com/2007/06/20/technology/20soft.html?_r=1&en=123a376f5de21afd&ei=5070&emc=eta1

From CNN.com:

AT&T anti-piracy effort raises privacy concerns

In a break with other Internet service providers, AT&T Inc. will work with Hollywood studios and recording labels to devise technology that identifies offshore content pirates who use its network to upload illegal copies of movies and music.

[FULL STORY](#)

Paranoia grows over Google's power

Most people missed the announcement about how Google wants to burrow inside your brain and capture your most intimate thoughts. That's because it never happened.

[FULL STORY](#)

Blockbuster backs Blu-ray

Blockbuster Inc. will rent high-definition DVDs only in the Blu-ray format in 1,450 stores when it expands its high-def offerings next month, dealing a major blow to the rival HD DVD format.

[FULL STORY](#)

Report: Parents would back limits on media violence, sex

Two-thirds of parents said they are very concerned about sex and violence the nation's children are exposed to in the media, and there would be broad support

for new federal limits on such material on television, said a survey released Tuesday.

[FULL STORY](#)

Users rage against China's 'Great Firewall'

Yang Zhou is no cyberdissident, but recent curbs on his Web surfing habits by China's censors have him fomenting discontent about China's "Great Firewall."

[FULL STORY](#)

Video game gets banned

British censors Tuesday banned a video game for the first time in 10 years, rejecting U.S.-published "Manhunt 2" for what they described as an unrelenting focus on sadism and brutal slaying.

[FULL STORY](#)

From the Christian Science Monitor:

A Briton who called himself "Son of God" was at the center of a global child pornography ring smashed by police after a 10-month investigation, authorities in London said Monday. The probe uncovered more than 75,000 images on Timothy Cox's computer of youths being subjected to sexual abuse, plus evidence that he'd supplied 11,000 more to users of his website. Cox has been in custody since last September. The authorities said more than 700 other suspects in 35 countries were arrested and 31 children had been "rescued."

Two-thirds of parents expressed deep concern about sex and violence in the media and voiced broad support for new federal limits to such material on television, according to a report released Tuesday by the Kaiser Family Foundation. About three-fourths rated exposure to inappropriate material as one of their top parental concerns.

Progress on preventing blackouts

Mandatory rules governing the reliability of the US power grid go into effect Monday. By Mark Clayton

<http://www.csmonitor.com/2007/0618/p02s01-ussc.html?s=hns>

In Second Life, no jail time for fictional crime

In a virtual world, punish misbehaving avatars, not the people behind them. By Jim Sollisch

<http://www.csmonitor.com/2007/0618/p09s02-coop.html?s=hns>

Universities strike back in battle over illegal downloads

With 1.3 billion music files pirated by college students last year, schools are turning to technology to curb the practice. Congress watches with interest. By Amy Brittain

<http://www.csmonitor.com/2007/0618/p13s01-legn.html?s=hns>

From Christian Computing:

Don't be a Bible Software Power User "Wanabe"

WordSEARCH Word - Bob Dasal

Your Bible software program contains the study tools you use to make your sermon preparation time productive. The software has more power than you know how to use so you want to become a power user. To Read The Entire Article, [Click Here!](#)

Data Security: Can You Back Up Your Backup Strategy?

ACS Ideas To Impact - Hal Campbell

Administrative personnel are overwhelmed every day with managing tremendous amounts of data electronically. Whether it's adding new members to the database or entering contribution amounts, church staff members depend heavily on their digital technology. To read the entire article, [Click Here!](#)

The Web 2.0 Revolution in Church Growth, Part 1

Special Feature - Mike Simson

Internet Web 2.0 technology may find its way into the history books as having as much, or more impact on the Christian landscape as the invention of Gutenberg's printing press in the 1440's. The printing press released the power of human communications and therefore changed human history, especially the Church as it made it possible for common people to have their own Bibles. Today, Christians all over the world are fast discovering the power of the internet, which may prove to be a ministry tool that revolutionizes the way we think about and do church for generations to come. To read the entire article, [Click Here!](#)

Malware Mayhem

Tech Talk - Dr. J.D. "Doc" Watson

Just to show you that even a seasoned computer user can get bit by intrusive software, this month I want to share with you how it happened to me, examine how to get rid of such stuff, and finally, more importantly, how to protect yourself from getting it again. To read the entire article, [Click Here!](#)

Can RSS Help Keep You Connected?

Higher Power with Kevin - Kevin Purcell

Really Simple Syndication, most often known as RSS and also known as Rich Site Summary is a great way to keep your readers, listeners or viewers up to date on the content you provide. And it is becoming a more popular form of Internet communication. To read the entire article, [Click Here!](#)

Online Scams: Work at Home and Summer Jobs

information Security - Ben Woelk

Proverbs often contrasts wisdom and foolishness. Online scammers hope we'll act foolishly. Most con-men used to prey on people by going door-to-door or over the phone. Now they've found it far easier to dangle their bait through the internet to thousands or even millions of potential victims. And they're making a lot of money! To read the entire article, [Click Here!](#)

Yvon has a channel on YouTube!

Ministry Communications - Yvon Prehn

We live in a time of multi-channel communication, where we have to get our message out in every imaginable way, this is a message I tell people in my seminars. But it's more than words to me as I constantly try new ways to communicate. My latest adventure is YouTube, and even if you don't want to read more check out the results at: www.youtube.com/yvonprehn. For some practical advice and how I did it, read on. To read the entire article, [Click Here!](#)

From Macworld.com:

First Look: Safari 3 beta

<http://www.macworld.com/2007/06/firstlooks/safari3/index.php?lsrc=mwweek>

Leopard preview: Desktop and Finder changes

<http://www.macworld.com/2007/06/firstlooks/desktopfinderfl/index.php?lsrc=mwweek>

Macworld Podcast: WWDC Roundtable

<http://www.macworld.com/weblogs/mwpodcast/2007/06/mwpodcast85/index.php?lsrc=mwweek>

Macworld Video: Safari 3

<http://www.macworld.com/weblogs/mwvodcast/2007/06/mwvodcast12/index.php?lsrc=mwweek>

Analysis: Safari move driven by iPhone, market share

<http://www.macworld.com/news/2007/06/11/safarianalysis/index.php?lsrc=mwweek>

iPhone users will need iTunes account, Apple says

<http://www.macworld.com/news/2007/06/13/iphoneitunes/index.php?lsrc=mwweek>

Instant iPhoto slideshows

<http://www.macworld.com/weblogs/macoshints/2007/06/iphotoslide/index.php?lsrc=mwhints>

A possible fix for slow iTunes search box typing

<http://www.macworld.com/weblogs/macoshints/2007/06/itunesstye/index.php?lsrc=mwhints>

From PCWorld.com:

Environmental Databases Unveiled

The National Oceanic & Atmospheric Administration is opening access to natural resources data for mashup.

http://www.pcworld.com/article/id,132975/article.html?tk=nl_dnxnws

Microsoft Drops Digital Image Suite

Functions for photo-organizing app are now bundled into the operating system.

http://www.pcworld.com/article/id,132992/article.html?tk=nl_dnxnws

Google Gears Draws Developers

Analysis: New Google browser plug-in offers offline access to Web-hosted applications, intriguing developers.

http://www.pcworld.com/article/id,132985/article.html?tk=nl_dnxnws

'Image Spam' Slips into Inbox

Scam images sent as stationery backgrounds are the latest tactic in ducking antispam filters.

[Read the story](#)

How to Set Up RAID on Your PC

Boost your hard-drive performance, add redundancy, or do both by converting your PC to use a RAID setup.

[Read the article](#)

Windows Tips: Accelerate Windows by Tweaking Virtual Memory

These tricks can pep up your computer; plus, download a free Mac OS X skin.

[Read the article](#)

Digicams Take to Water

Underwater photography goes digital with a selection of compact, capable, budget cameras.

http://www.pcworld.com/article/id,132916/article.html?tk=nl_dnxnws

Apple Improves iPhone Battery, Screen Cover

Apple announced on Monday improvements to the battery life and the the top surface of the iPhone's display.

http://www.pcworld.com/article/id,133008/article.html?tk=nl_dnxnws

25 Web Sites to Watch

What's tomorrow's YouTube? The Web's next breakout hit may be one these innovative, useful, and fun new sites.

http://www.pcworld.com/article/id,132787/article.html?tk=nl_dnxnws

Virtual Computing: Still a Learning Experience

The popular technology promises to make computing easier, but it takes time to get up to speed.

http://www.pcworld.com/article/id,132993/article.html?tk=nl_dnxnws

19 Million Americans Interested in Buying iPhone

Market research firm M:Metrics reports that 19 million Americans have a strong interest in purchasing the device.

http://www.pcworld.com/article/id,133005/article.html?tk=nl_dnxnws

Former Enron Broadband CEO Sentenced

The former chief executive officer of Enron Broadband Services has been

sentenced to 27 months in prison on securities fraud charges, the U.S. Department of Justice announced today.

http://www.pcworld.com/article/id,133022/article.html?tk=nl_dnxnws

Google Launches Public Policy Blog

Google has launched a blog focused on U.S. government legislation and regulation.

http://www.pcworld.com/article/id,133031/article.html?tk=nl_dnxnws

Dell Says 'We Blew It' When Bullying Blog

A Dell manager said his company was wrong to threaten a blog for posting great bargain-hunting tips.

http://www.pcworld.com/article/id,133041/article.html?tk=nl_dnxnws

Businesses Experimenting With Virtual Worlds

Many companies are already dabbling in one or more virtual worlds or closely observing them.

http://www.pcworld.com/article/id,133025/article.html?tk=nl_dnxnws

'Italian Job' Web Attack Sweeping the 'Net

Tens of thousands of legitimate Web sites now function as weapons for Internet criminals, security vendors said Monday.

http://www.pcworld.com/article/id,133042/article.html?tk=nl_dnxnws

Linux Supporters: Microsoft's Patent Threats Baseless

Attendees of the first Linux Foundation Summit aren't worried by Microsoft's threats to sue customers for patent infringement.

http://www.pcworld.com/article/id,133060/article.html?tk=nl_dnxnws

Europe Awaits Apple Response to Antitrust Charges

Apple and four of the biggest record companies this week must submit written responses to antitrust charges that they restricted online sales of music in Europe.

http://www.pcworld.com/article/id,133038/article.html?tk=nl_dnxnws

Microsoft Sets July 1 as Office 2003 Cutoff

Microsoft says it will pull the plug on Office 2003 for PC builders on June 30.

http://www.pcworld.com/article/id,133046/article.html?tk=nl_dnxnws

Is Google Too Big?

With its empire expanding, the search giant can have an unprecedented breadth of knowledge about you. Can we trust it with so much data?

http://www.pcworld.com/article/id,132989/article.html?tk=nl_dnxnws

Stop Users Before They Click on Risky Web Sites

In a MIT-Harvard study, 36 percent of subjects logged in to their online bank accounts despite being warned that the site was not secure.

http://www.pcworld.com/article/id,133066/article.html?tk=nl_dnxnws

From ITBusiness Edge:

[Open Source and the CIO](#) :: silicon.com

[Linux Foundation Answers Microsoft Patent Threat](#) :: BusinessWeek

[Linux Creator Linus Torvalds Unimpressed with GPLv3](#) :: InformationWeek

[Badbunny Infecting Operating Systems](#) :: ZDNet

From Techtarget.com:

How routers work

<http://go.techtarget.com/r/1607181/5300425>

TCP/IP troubleshooting: A structured approach

<http://go.techtarget.com/r/1607182/5300425>

Wireless Internet access -- 3G vs. Wi-Fi

<http://go.techtarget.com/r/1607183/5300425>

VLANs -- Controlling wired and wireless traffic

<http://go.techtarget.com/r/1607189/5300425>

For a complete list of wireless answers go to Lisa's expert page:

<http://go.techtarget.com/r/1607196/5300425>

Network disaster recovery tips for business continuity

Network disaster recovery planning tips for business continuity from Verizon

Business highlight what needs to be done to weather the storm.

<http://go.techtarget.com/r/1607201/5300425>

Summer isn't just about lemonade and barbecues. So how can you ensure that your SMB remains secure and safe in the midst of a disaster? We can help.

<http://go.techtarget.com/r/1607669/5300425>

Laptops can free employees to work remotely, allowing them to telecommute and travel easily. But that freedom comes with security perils.

<http://go.techtarget.com/r/1607670/5300425>

Microsoft is lining up Linux partners to maintain the dominance of its operating system. But will it work?

<http://go.techtarget.com/r/1617883/5300425>

From Microsoft:

[What's the difference between spyware and a virus?](#)

Both are unwanted or malicious software, sometimes called "malware." Find out how they're different and how you can protect yourself from both.

[Back up your files](#)

If you only do one maintenance task on your PC, make it this one. Keep copies of your important files in case something happens to your PC.

WHITE PAPERS:

TITLE: "Solving the Weakest Link in Network Security: Passwords"

<http://go.techtarget.com/r/1602058/3976660>

PUBLISHER: DigitalPersona

Electronic document retention and destruction: The impact of global regulations -
- IT Briefing

Published by: CA Inc.

<http://go.techtarget.com/r/1606869/5300425>

SECURITY News:

From SANS:

--Anti-Spyware Bill Introduced in US Senate

(June 15, 2007)

US Senator Mark Pryor (D-Arkansas) has introduced legislation that would make it a crime to install spyware on PCs without users' consent. Pryor said he took the step of introducing the Counter Spy Act of 2007 because "the industry has failed in self-regulating." The bill would make it an unfair practice to install spyware. The bill would also give the Federal Trade Commission (FTC) enforcement powers. Violators could face civil and criminal penalties, which could be both fines and prison sentences of up to five years.

<http://www.informationweek.com/shared/printableArticle.jhtml?articleID=199904803>

http://news.com.com/8301-10784_3-9729925-7.html

<http://pryor.senate.gov/newsroom/details.cfm?id=276980&>

--PayPal Deploys Two-Factor Authentication

(June 18, 2007)

PayPal users will now have an extra layer of security to use when accessing their accounts. A key fob token generates a "pseudo-random six-digit" security passcode every 30 seconds. The device is available to both PayPal customers and eBay customers; eBay is the parent company of PayPal. PayPal and eBay top most lists of frequent phishing targets. Customers will need to pay a US \$5 fee for the device, but beyond that, the service costs nothing.

<http://www.securityfocus.com/brief/528>

[Editor's Note (Ranum): Fantastic!!!! They'll get my \$5. (Shpantzer): I'm all for strong authentication. One niggling issue is the possibility that companies that give tokens to customers would use them as an excuse to not refund lost monies in the event of true fraud. Non-repudiation (via strong authentication) could possibly be used against fraud victims by saying 'Hey, we gave you a token,. Who else could it have been but you? No refund!']

FROM SNOPE.COM:

- Photograph shows "[God's hands](#)" in a cloud formation.

- Should an American flag be [burned](#) if it has been allowed to touch the ground?
- Will adding [acetone](#) to gasoline improve an automobile's mileage?
- Photograph purports to show a [split tongue](#) body modification with a zipper installed.
- Photographs show wild [bears](#) posing with humans on the grounds around a cottage in Alaska.
- Hoax article claims [Paris Hilton](#) has been stabbed several times in the jail where she is serving out her sentence.

Worth a Second Look

- We examine the claim that more [collect](#) phone calls are made on Father's Day than on any other day of the year.

Still Haunting the Inbox

- Yes, ingestion of [hand sanitizer](#) by children can result in alcohol poisoning.
- The saga of [Hogzilla](#), the giant boar - how big it was, where it was, who shot it, and why.
- No, [Jay Leno](#) did not write the "Hits the Nail on the Head" essay — it was Craig R. Smith.
- About "strawberry quick," a candied form of [methamphetamine](#), and the danger it poses to children.
- Petition advocates buying/not buying gasoline from [Citgo](#). And no, Citgo did not change its name to Petro Express.
- There was no letter to [Starbucks](#) from coffee-seeking G.I.s serving in Iraq, so no response from the coffee retailer saying it didn't support the war and anyone in it. As for Oscar Meyer refusing troops free hot dogs, the 2004 Starbucks e-mail was altered in 2007 to aim it at the blameless hot dog maker.
- A 4-year-old British girl named [Madeleine McCann](#) is missing from a Portuguese resort.
- No, robbers are not luring female victims into sniffing ether-laced [perfume](#) in parking lots.
- E-mailed petition advocates [denying](#) social services to immigrants.
- The missing child alert about 13-year-old [Ashley Flores](#) of Philadelphia is a hoax.
- [809 area code scam](#): Unsuspecting phone customers have been gulled by con artists into placing calls to area codes in the Caribbean that result in hefty charges.
- The entreaty to aid 7-year-old [Amy Bruce](#) who is dying of lung cancer and a brain tumor by forwarding an email and a sappy poem titled "Slow Dance" is a hoax.
- Godless soda cans: Someone has confused Pepsi with Dr Pepper. Dr Pepper's "one nation" can design that omitted "[under God](#)" from a quote from the Pledge of Alligiance was used for only a short time ending in February 2002. The cans haven't been on the shelves since. Newer versions of incitements to boycott name Pepsi as the culprit responsible

for Godless cans, but this is just a garbling of the Dr Pepper story — Pepsi has nothing to do with this.

- Dialing [#77 or *677](#) is not a surefire way of reaching the local highway patrol — the service is in place in some regions, but not in others. If in need of assistance, dial 911 instead for the sure thing.
- While it is true that in 2004 a man in India was electrocuted when trying to use his cell phone as it recharged, it is safe to use your cell phone while it is [charging](#).
- The Internet-circulated list of five little-known but useful [cell phone functions](#) contains some truth, some falsehoods, and some half-truths. And no, you won't unleash "hidden battery power" by keying in *3370#.
- While actor [Lee Marvin](#) did fight in the Pacific theater during World War II, earned a Purple Heart, and is buried in Arlington National Cemetery, he and Bob Keeshan (TV's "Captain Kangaroo,") did not fight together in the battle for Iwo Jima.
- Will pressing [#-9-0](#) on your telephone allow scammers to make long-distance calls and charge them to your phone bill?
- No, reusing [plastic bottles](#) will not result in their breaking down into cancer-causing components.
- [Hillary Clinton](#) is the subject of many e-mailed items, and our "Clintons" section contains write-ups about a number of them.
- No, [Bill Gates](#) is not sharing his fortune with everyone who forwards a specific e-mail on his behalf. This tired leg-pull continues to romp through everyone's inbox, the [most widespread incarnation](#) swearing "This took two pages of the Tuesday USA Today!"
- [Virus](#) announcement and virus hoax e-mails are afoot! We try to keep current on them and do our best to point readers to authoritative links confirming or debunking them.

Fraud Afoot

- Seems like everyone has become the recipient of mysterious e-mails promising untold wealth if only one helps a wealthy foreigner quietly move millions of dollars out of his country. The venerable [Nigerian Scam](#) has discovered the goldmine that is the Internet. Beware — there's still no such thing as "something for nothing," and the contents of your bank account will end up with these wily foreigners if you fall in with this.
- Likewise, look out for mailings announcing you've won a foreign [lottery](#) you don't recall entering.
- Or that because you share the surname of a wealthy person who died without leaving a will you're in line for a windfall [inheritance](#).
- And be especially wary if, while trying to sell or rent anything online (car, boat, horse, motorcycle, painting, apartment, you name it) you're approached by a prospective buyer/renter who wants to pay with a cashier check made out for an amount [in excess](#) of the agreed-upon price and who asks the balance be sent to a third party.
- Aspiring [work-at-homers](#) promised big bucks for acting as intermediaries for international transactions wherein they cash checks for other parties or

reship goods to them have been defrauded by con artists. Don't you be next.

- If someone telephones to announce you can have a \$200 Wal-Mart [shopping spree](#) or \$200 in [gasoline coupons](#) in return for a \$3.49 processing charge to be debited directly from your bank account, hang up. You're being set up via the promise of "something for almost nothing" into authorizing a swindler to help himself to the contents of your bank account.
- If someone calls to announce you've failed to appear for [jury duty](#) and will be arrested, do not give the caller your personal and financial information in an effort to prove he's sending the gendarmes after the wrong guy. You're being tricked into giving up this information to an identity thief.

WORMS, ACTIVE EXPLOITS, VULNERABILITIES & PATCHES

From SANS:

CRITICAL: Microsoft Windows Schannel Remote Code Execution (MS07-031)

Affected:

Microsoft Windows 2000

Microsoft Windows XP

Microsoft Windows Server 2003

Description: The Microsoft Windows Secure Channel (Schannel) subsystem is the Microsoft Windows implementation of the Internet-standard Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. These protocols are used for cryptographically secure communications across the Internet. This subsystem contains a flaw in the handling of cryptographic signatures. A specially-crafted signature sent by a server could trigger a remote code execution vulnerability. Any application utilizing the SSL or TLS protocols via the Schannel subsystem is potentially vulnerable; this includes Internet Explorer. This vulnerability could be exploited by a malicious web site. Full technical details for this vulnerability are publicly available.

Status: Microsoft confirmed, updates available.

Council Site Actions: All of the reporting council sites plan to distribute the updates during their next regularly schedule system maintenance cycle.

References:

Microsoft Security Bulletin

<http://www.microsoft.com/technet/security/Bulletin/MS07-031.mspx>

Posting by Thomas Lim

<http://www.securityfocus.com/archive/1/471203>

Wikipedia Articles on SSL and TLS

http://en.wikipedia.org/wiki/Secure_Sockets_Layer

http://en.wikipedia.org/wiki/Transport_Layer_Security

SecurityFocus BID

<http://www.securityfocus.com/bid/24416>

CRITICAL: Microsoft Internet Explorer Multiple Vulnerabilities (MS07-033)

Affected:

Microsoft Windows 2000
Microsoft Windows XP
Microsoft Windows Server 2003
Microsoft Windows Vista
Microsoft Internet Explorer 6
Microsoft Internet Explorer 7

Description: Microsoft Internet Explorer contains multiple vulnerabilities. Flaws in the handling of Microsoft Component Object Model (COM) objects, Cascading Style Sheets (CSS), Microsoft language packs, JavaScript scripts, and the Microsoft Speech Control could allow a specially-crafted web page to execute arbitrary code with the privileges of the current user. Additionally, a specially-crafted web page could exploit a flaw in the browser's "Navigation Canceled" page. Exploiting this flaw would allow an attacker to display arbitrary content in the context of that page, including script content. Any scripts executed in this page would execute with elevated privileges as compared to scripts in remote web pages. Some technical details for these vulnerabilities are publicly available. Status: Microsoft confirmed, updates available.

Council Site Actions: All of the reporting council sites plan to distribute the updates during their next regularly schedule system maintenance cycle.

References:

Microsoft Security Bulletin

<http://www.microsoft.com/technet/security/bulletin/ms07-033.msp>

Zero Day Initiative Advisories

<http://zerodayinitiative.com/advisories/ZDI-07-038.html>

<http://zerodayinitiative.com/advisories/ZDI-07-037.html>

SecurityFocus BIDs

<http://www.securityfocus.com/bid/24372>

<http://www.securityfocus.com/bid/24423>

<http://www.securityfocus.com/bid/24429>

<http://www.securityfocus.com/bid/24418>

<http://www.securityfocus.com/bid/22966>

<http://www.securityfocus.com/bid/24426>

CRITICAL: Microsoft Outlook Express and Windows Mail Multiple Vulnerabilities (MS07-034)

Affected:

Microsoft Windows XP

Microsoft Windows Server 2003

Microsoft Windows Vista

Description: Microsoft Outlook Express and Microsoft Windows Mail contain multiple vulnerabilities. Failure to properly validate local Universal Naming Convention (UNC) paths in email messages could allow a specially crafted email to execute arbitrary commands if the user clicks on a link in that email.

Additionally, a web page containing a specially crafted MIME HTML (MHTML) link could trigger a cross-site scripting vulnerability. Note that this flaw can be exploited from a web browser. Two additional information disclosure vulnerability applications were patched as part of this security bulletin. Some technical details are publicly available for these vulnerabilities.

Status: Microsoft confirmed, updates available.

Council Site Actions: All of the reporting council sites plan to distribute the updates during their next regularly schedule system maintenance cycle.

References:

Microsoft Security Bulletin

<http://www.microsoft.com/technet/security/bulletin/ms07-034.msp>

Wikipedia Article on MHTML

<http://en.wikipedia.org/wiki/MHTML>

SecurityFocus BIDs

<http://www.securityfocus.com/bid/17717>

<http://www.securityfocus.com/bid/23103>

<http://www.securityfocus.com/bid/24392>

<http://www.securityfocus.com/bid/24410>

HIGH: Microsoft Win32 API Remote Code Execution (MS07-035)

Affected:

Microsoft Windows 2000

Microsoft Windows XP

Microsoft Windows Server 2003

Description: Microsoft Windows's "Win32" application programming interface (API) contains a flaw in validating certain parameters passed to functions. The exact functions are not known, but Microsoft has confirmed that Internet Explorer calls the vulnerable functions in such a way as to be vulnerable to this attack. Any other application that uses these functions would likely be vulnerable as well. A specially-crafted web page could trigger the flaw in Internet Explorer; other vectors are possible through other applications. Successfully exploiting this vulnerability would allow an attacker to execute arbitrary code in the context of the vulnerable application.

Status: Microsoft confirmed, updates available.

Council Site Actions: All of the reporting council sites plan to distribute the updates during their next regularly schedule system maintenance cycle.

References:

Microsoft Security Bulletin

<http://www.microsoft.com/technet/security/Bulletin/ms07-035.msp>

SecurityFocus BID

<http://www.securityfocus.com/bid/24370>

HIGH: Microsoft Visio Multiple Vulnerabilities (MS07-030)

Affected:

Microsoft Visio 2002

Microsoft Office 2003

Description: Microsoft Visio, Microsoft's diagramming suite, contains multiple vulnerabilities. A specially-crafted Visio file containing an invalid version number or malformed packed object could trigger memory corruption vulnerabilities. Successfully exploiting these vulnerabilities would allow an attacker to execute arbitrary code with the privileges of the current user. Note that, depending upon configuration, Visio files may be opened without prompting.

Status: Microsoft confirmed, updates available.

Council Site Actions: All of the reporting council sites plan to distribute the updates during their next regularly schedule system maintenance cycle.

References:

Microsoft Security Bulletin

<http://www.microsoft.com/technet/security/Bulletin/MS07-030.msp>

SecurityFocus BIDs

<http://www.securityfocus.com/bid/24349>

<http://www.securityfocus.com/bid/24384>

--Yahoo! Fixes Cross-Site Scripting Flaw

(June 15, 2007)

Yahoo! has fixed a cross-site scripting flaw that could be exploited to take control of users' accounts. The flaw affected the entire Yahoo! site; attackers could exploit the flaw by tricking users into clicking on specially crafted links. The vulnerability is not dependent on a particular browser. Attackers could exploit the flaw to access address books, send email and instant messages, and review query histories and settings in various Yahoo! services.

http://www.theregister.co.uk/2007/06/15/yahoo_xss_error/print.html

[Editor's Note (Skoudis): Keep an eye on these Cross-Site Scripting (XSS) flaws. I think they are going to be very big in the future, especially as more users store more data online in so-called Web 2.0 applications. As the Sammy worm showed in MySpace two years ago, a determined XSS attacker could unleash a plague that steals or destroys data from millions of users. To help protect yourself, create a local back-up of the information you store in social networking, blogging, on-line photo, and even on-line e-mail accounts.

(Shpantzer): Note that this is a browser-independent issue. Moving away from Microsoft's Internet Explorer won't save us from basic coding flaws in the web's most popular platforms.]

Kat Lehman

Information Technology Coordinator

Diocese of Bethlehem

610-691-5655 x235

klehman@diobeth.org