



SECURITY BULLETIN

Content

- 1.....Information Security Guide for small business
- 2.....Security Alert
- 5.....Hot News

Free SMS Service

SMS Alert Service is a FREE value-added service. You can receive updated security alert anywhere and anytime to allow you responding timely.



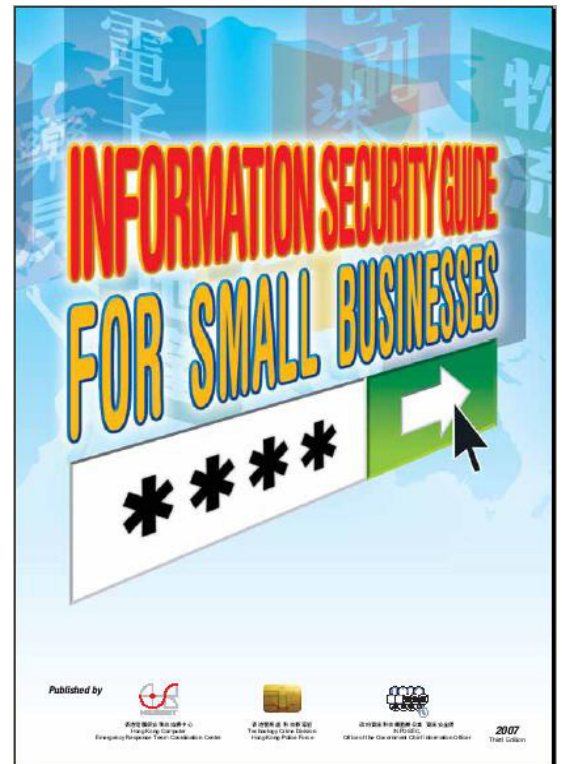
Please visit HKCERT web-site for more details:

https://www.hkcert.org/english/subscribe_ssl.html

Information Security Guide for small business

HKCERT, OGCIO and Hong Kong Police Force has published the third edition of SME information security guide. It added information on business continuity planning facing by small and medium enterprises.

The guide is now available at HKCERT's website, which can be reached via the following link:



http://www.hkcert.org/english/sguide_faq/sguide/sme_guideline.pdf

Security Alert

Bugs, Holes and Patches					
Date/Source	Common Name	Operating system/ Vendor/ Platform	Vulnerability System	Impact	Workarounds/ Solutions
2008/09/01	Novell Forum TCL Command Injection Vulnerability	Novell	- Novell Forum (formerly SiteScape Forum) 7.x - Novell Forum (formerly SiteScape Forum) 8.x	- Remote Code Execution	Install the patch provided by manufacturer. Please visit our web-site for more details. http://www.hkcert.org
2008/09/02	Novell eDirectory Multiple Vulnerabilities	Novell	- Novell eDirectory version 8.8	- Remote Code Execution	Install the patch provided by manufacturer. Please visit our web-site for more details. http://www.hkcert.org
2008/09/02	VMware Products Multiple Vulnerabilities	VMware	- VMware Server 1.x - VMware Workstation 5.x and 6.x - VMware Player 1.x and 2.x - VMware ACE 1.x and ACE 2.x - VMware Fusion 1.x	- Remote Code Execution - Denial of Service - Privileges Escalation	Install the patch provided by manufacturer. Please visit our web-site for more details. http://www.hkcert.org
2008/09/04	Novell iPrint Client "IppCreateServerRef" Buffer Overflow Vulnerability	Windows	- Novell iPrint Client version 4.36 and prior - Novell iPrint Client version 5.06 and prior	- Remote Code Execution	Install the patch provided by manufacturer. Please visit our web-site for more details. http://www.hkcert.org
2008/09/10	Microsoft Office Uniform Resource Locator Validation Error Vulnerability (10 September 2008)	Windows	- Microsoft Office XP - Microsoft Office 2003 - 2007 Microsoft Office System - Microsoft Office OneNote 2007	- Remote Code Execution	Install the patch provided by manufacturer. Please visit our web-site for more details. http://www.hkcert.org
2008/09/10	Microsoft Windows Media Encoder Buffer Overrun Vulnerability (10 September 2008)	Windows	- Windows Media Encoder 9 Series - Windows 2000 - Windows XP - Windows Server 2003 - Windows Vista - Windows Server 2008	- Remote Code Execution	Install the patch provided by manufacturer. Please visit our web-site for more details. http://www.hkcert.org

Bugs, Holes and Patches					
Date/Source	Common Name	Operating system/ Vendor/ Platform	Vulnerability System	Impact	Workarounds/ Solutions
2008/09/10	Microsoft Products GDI+ Multiple Vulnerabilities (10 September 2008)	Windows	<ul style="list-style-type: none"> - Windows XP - Windows Server 2003 - Windows Vista - Windows Server 2008 - Microsoft Windows 2000 - Microsoft Internet Explorer 6 - Microsoft .NET Framework 1.0 - Microsoft .NET Framework 1.1 - Microsoft .NET Framework 2.0 - Microsoft Office XP - Microsoft Office 2003 - 2007 Microsoft Office System - Microsoft Visio 2002 - Microsoft Office PowerPoint Viewer 2003 - Microsoft Works 8 - Microsoft Digital Image Suite 2006 - SQL Server 2000 Reporting Services - SQL Server 2005 - Microsoft Visual Studio .NET 2002 - Microsoft Visual Studio .NET 2003 - Microsoft Visual Studio 2005 Service Pack 1 - Microsoft Visual Studio 2008 - Microsoft Report Viewer 2005 Service Pack 1 Redistributable Package - Microsoft Report Viewer 2008 Redistributable Package - Microsoft Visual FoxPro 8.0 when installed on Microsoft Windows 2000 Service Pack 4 - Microsoft Visual FoxPro 9.0 when installed on Microsoft Windows 2000 Service Pack 4 - Microsoft Platform SDK Redistributable: GDI+ - Microsoft Forefront Client Security 1.0 when installed on Microsoft Windows 2000 Service Pack 4 	- Remote Code Execution	Install the patch provided by manufacturer. Please visit our web-site for more details. http://www.hkcert.org
2008/09/10	Microsoft Windows Media Player Sampling Rate Vulnerability (10 September 2008)	Windows	<ul style="list-style-type: none"> - Windows Media Player 11 Windows XP Windows Vista Windows Server 2008 	- Remote Code Execution	Install the patch provided by manufacturer. Please visit our web-site for more details. http://www.hkcert.org
2008/09/11	Apple QuickTime Multiple Remote Code Execution Vulnerabilities	All	- Apple QuickTime versions prior to 7.5.5	<ul style="list-style-type: none"> - Denial of Service - Remote Code Execution 	Install the patch provided by manufacturer. Please visit our web-site for more details. http://www.hkcert.org
2008/09/16	Apple iPhone Multiple Vulnerabilities	iPhone	- Apple iPhone versions 1.0 through 2.0.2	<ul style="list-style-type: none"> - Denial of Service - Remote Code Execution - Bypass Security Restrictions - Poison DNS cache 	Install the patch provided by manufacturer. Please visit our web-site for more details. http://www.hkcert.org

Bugs, Holes and Patches					
Date/Source	Common Name	Operating system/ Vendor/ Platform	Vulnerability System	Impact	Workarounds/ Solutions
2008/09/17	Apple Mac OS X Multiple Vulnerabilities	Mac	<ul style="list-style-type: none"> - Apple Mac OS X version 10.4.11 and prior - Apple Mac OS X Server version 10.4.11 and prior - Apple Mac OS X versions 10.5 through 10.5.4 - Apple Mac OS X Server versions 10.5 through 10.5.4 	<ul style="list-style-type: none"> - Remote Code Execution - Disclose Sensitive Information - Security Bypass - Denial of Service 	Install the patch provided by manufacturer. Please visit our web-site for more details. http://www.hkcert.org
2008/09/18	Adobe Illustrator Unspecified Code Execution Vulnerabilities	Mac	<ul style="list-style-type: none"> - Adobe Illustrator CS2 for Mac 	<ul style="list-style-type: none"> - Remote Code Execution 	Install the patch provided by manufacturer. Please visit our web-site for more details. http://www.hkcert.org
2008/09/22	VMware ESX and ESXi Openwsman Buffer Overflow Vulnerabilities	VMware	<ul style="list-style-type: none"> - VMware ESXi versions 3.x - VMware ESX versions 3.x 	<ul style="list-style-type: none"> - Denial of Service - Remote Code Execution 	Install the patch provided by manufacturer. Please visit our web-site for more details. http://www.hkcert.org
2008/09/25	Mozilla Products Multiple Vulnerabilities	All	<ul style="list-style-type: none"> - Mozilla Firefox versions prior to 3.0.2 - Mozilla Firefox versions prior to 2.0.0.17 - Mozilla Thunderbird versions prior to 2.0.0.17 - Mozilla SeaMonkey versions prior to 1.1.12 	<ul style="list-style-type: none"> - Denial of Service - Disclose Sensitive Information - Remote Code Execution - Security Bypass 	Install the patch provided by manufacturer. Please visit our web-site for more details. http://www.hkcert.org
2008/09/25	Cisco IOS Linecard Redundancy Unauthorized Access Vulnerability	Cisco	<ul style="list-style-type: none"> - Cisco IOS Software Release 12.2BC - Cisco IOS Software Release 12.2CX - Cisco IOS Software Release 12.2CY - Cisco IOS Software Release 12.2XF - Cisco IOS Software Release 12.3BC 	<ul style="list-style-type: none"> - Unauthorized Access: Privilege Escalation 	Install the patch provided by manufacturer. Please visit our web-site for more details. http://www.hkcert.org
2008/09/26	Mac OS X Java Multiple Vulnerabilities	Mac	<ul style="list-style-type: none"> - Apple Macintosh OS X 	<ul style="list-style-type: none"> - Denial of Service - Disclose Sensitive Information - Remote Code Execution - Security Bypass 	Install the patch provided by manufacturer. Please visit our web-site for more details. http://www.hkcert.org

* Please check instructions carefully on related web site before applying the solutions

Hot News

Neo-Nazi forum hacked *September 01, 2008*

German anti-fascist hackers have broken into the secure forum server of one of the world's largest neo-Nazi groups, Blood & Honour, and copied more than 30,000 pieces of data.

Blood & Honour, founded back in 1987 in the UK by Ian Stuart Donaldson, leader of the notorious skinhead band Skrewdriver, has been banned in Germany since 2000. The Spanish division was closed in 2005 after the arrest of many of its main leaders.
(from The Register)

Zombie network explosion *September 02, 2008*

The number of compromised zombie PCs in botnet networks has quadrupled over the last three months, according to figures from the Shadowserver Foundation.

It could be that experienced botnet herders have got better at keeping control of compromised machines, or that more machines have been infected. Not much by way of email malware activity has been monitored, so if the latter explanation is true, then drive-by download attacks are playing a bigger role in spreading botnet client infestation. The recent rise in SQL injection attacks that plant malicious scripts on vulnerable servers could be to blame, but there's no hard data to support this plausible theory.
(from The Register)

Spammers use free Web services to shield harmful links *September 03, 2008*

Spammers are abusing free Web services to make their spam links look more legitimate, according to e-mail security vendor MessageLabs Ltd.

One of the services, a photo hosting site called ImageShack, lets people upload different types of photo formats, including Flash files, said Paul

Wood, a senior analyst at MessageLabs.

Flash files, which have the extension ".swf," can be used for animated graphics and to automatically redirect people to other Web sites — a feature that can be abused.
(from Computer World)

Open source release takes Linux rootkits mainstream *September 04, 2008*

The art of burying invisible malware deep inside a Linux machine is about to go mainstream, thanks to a new open-source rootkit released Thursday by Immunity Inc., a firm that supplies tools for penetration testers.

When implemented, Immunity's DR, or Debug Register, makes backdoors and other types of malware extremely difficult to detect or eradicate. It's notable because it cloaks itself by burrowing deep inside a server's processor and availing itself of debugging mechanisms available in Intel's chip architecture. The rootkit, in other words, mimics a kernel debugger.
(from The Register)

FCC warns of new phishing scam *September 05, 2008*

The US Federal Communications Commission (FCC) is warning businesses to be on the lookout for a new spam run impersonating its Fee Filer payment system.

The FCC said in a statement (PDF) that a new phishing attack is attempting to dupe companies into handing over financial details through bogus regulatory payments.
(from Vnunet)

Facebook botnet risk revealed *September 06, 2008*

Researchers have created a proof-of-

concept application for Facebook that turned the machines of people who added the app to their Facebook page into elements of a botnet that in a demonstration launched denial-of-service attacks on a victim server.

The demo application, called "Photo of the Day," displays a new photo from *National Geographic* every day. However, every time someone views the photo, the host computer is forced "to serve a request of 600 Kbytes," according to the paper.
(from CNET)

Google reveals Chrome security patch details *September 08, 2008*

Earlier today, Google was keeping mum about a three-day-old security fix to its Chrome browser, but now the company has revealed details of two critical-risk vulnerabilities and some lesser issues it says are fixed.

The critical patches relate to buffer overrun vulnerabilities that could have let a remote attacker execute arbitrary software on a Chrome user's computer, said Mark Larson, a Google Chrome program manager, in a mailing list posting Monday afternoon. The first patch fixed a vulnerability in handling long file names, called the SaveAs vulnerability, and the second a vulnerability in dealing with the Web site addresses displayed in Chrome's status area when the user hovers over a link.
(from CNET)

Obama strumpet-sex scandal ruse spreads malware *September 09, 2008*

False claims that presidential candidate Barack Obama is a sex tourist are being used to trick users into getting infected by malware.

Prospective marks are encouraged to check out a video implausibly showing the married Democrat in action with a Ukrainian strumpet. Gullible folks who

fall for the ruse are shown a bongo clip while, in the background, malicious files are installed onto their Windows PCs, net security firm Websense reports.

(from *The Register*)

Apple code of secrecy imperils Aunt Mildred

September 10, 2008

Those who use Apple's iTunes or QuickTime on either a Mac or Windows machine, or who own an iPod touch, will want to install newly released updates that fix a raft of serious security bugs. Not that Apple is going out of its way to warn of the risks, mind you.

The most serious of the batch seem to be updates for QuickTime, which plug holes that could allow attackers to hijack a Mac or PC simply by tricking a user into viewing a maliciously crafted video or picture. (And given the presence of millions of recently compromised websites, how hard can that be?)

(from *The Register*)

CookieMonster nabs user creds from secure sites

September 11, 2008

Dubbed CookieMonster, the toolkit is used in a variety of man-in-the-middle scenarios to trick a victim's browser into turning over the authentication cookies used to gain access to user account sections of a website. Unlike an attack method known as sidejacking, it works with vulnerable websites even when a user's browsing session is encrypted from start to finish using the secure sockets layer (SSL) protocol.

According to Mike Perry, the creator of CookieMonster, websites that appear to be vulnerable to the attack include united.com, bankofamerica.com, register.com, netflix.com, and a host of other big-name online destinations. Errata Security's Rob Graham, who introduced Sidejacking tools a little more than a year ago, says Gmail is not vulnerable as long as a recently implemented https-only option is turned on. But Google Docs, Google's

Blogger.com and Google Finance remain wide open.

(from *The Register*)

Hackers hit Large Hadron Collider Web site

September 12, 2008

Hackers defaced one of the Web sites of the Large Hadron Collider (LHC) earlier this week, but the controversial science project's network suffered no permanent damage, a spokesman for CERN maintained today.

The hackers targeted a site for the Compact Muon Solenoid (CMS), one of the major experiments being run at the LHC. Built around a huge solenoid magnet that generates a magnetic field 100,000 times more powerful than Earth's own, the CMS detector is designed to search for the Higgs boson particle and others that could make up the elusive dark matter scientists theorize comprises the bulk of the universe's matter.

(from *Computer World*)

Virginia de-convicts AOL junk mailer Jeremy Jaynes

September 13, 2008

Notorious American AOL spammer Jeremy Jaynes had his nine year federal prison sentence overturned today, when Virginia's high court ruled the state's tough "anti-spam" law violates the First Amendment right to free speech.

Jaynes, a resident of North Carolina, was convicted in 2004 of three counts of junk email offenses by spamming tens of thousands of AOL users by means of a stolen database containing around 100 million addresses. He was once rated as the eighth worst spammer in the world by the anti-spam firm Spamhouse and is the first American to be convicted of a felony for sending unsolicited bulk email.

(from *The Register*)

'BusinessWeek' site hacked in potential malware attack

September 15, 2008

Hackers have broken into *BusinessWeek's* online site and set up

an attack scenario in which visitors to a section of the site could have their own computers compromised and their data stolen, a security researcher said on Monday.

The hackers used an increasingly common form of attack called SQL injection, in which a small malicious script is inserted into a database that feeds information to the *BusinessWeek* Web site, he said. The executable code in the database links to a Web site with a Russian domain, which could download malware onto the computers of *BusinessWeek.com* readers.

(from *CNET*)

McAfee: Brad Pitt fan sites may be bad for your computer

September 16, 2008

According to McAfee's new "riskiest celebrities in cyberspace" list, when searching for "Brad Pitt," "Brad Pitt downloads," or Brad Pitt wallpaper, screen savers, and pictures, Internet users experience an 18 percent chance of stumbling upon sites containing malicious code. This includes drive-by malware that can infect your PC without asking you to download anything. Such social engineering, once reserved for e-mail, is now being used to populate search results with fake sites for these personalities.

One site advertising Angelina Jolie downloads, for example, contained 978 hidden malware-infected wallpaper and photo downloads, said McAfee. A site dedicated to Jessica Alba linked to other bad sites, contained misleading offers to gather information and produced a high number of spam e-mails when an e-mail address was provided.

(from *CNET*)

Update: Hackers claim to break into Palin's Yahoo Mail account

September 17, 2008

A group of hackers that hit the Church of Scientology's site earlier this year have apparently cracked the Yahoo Mail account belonging to Gov. Sarah Palin, the Republican nominee for vice president, according to documents and screenshots posted on the Web.

A security expert called the practice of using private e-mail accounts "incredibly dangerous" for public officials such as Palin.
(from Computer World)

Security researchers ponder possible Palin hacks
September 18, 2008

Security experts speculating today on how Alaska Gov. Sarah Palin's Yahoo e-mail account had been hacked put forward several theories, with some skeptical of claims that the access was gained by a simple password reset.

Yahoo users who ask the service to remind them of their password are asked for just a few personal details -- such as birth date, country of residence and postal code -- but assuming those are entered correctly, the password is e-mailed to an alternate account, which has had to be entered previously. Computerworld's tests today, which involved several accounts and used various combinations of password reset queries, always resulted in the Yahoo password or username being sent to an alternate address. However, if a user says his or her alternate e-mail address is unavailable, the password can be reset.
(from Computer World)

Yahoo, Hotmail, Gmail all vulnerable to Palin-style password-reset hack
September 19, 2008

Yahoo Mail isn't the only Web-based mail service that could be duped into giving up someone else's account password, the tactic that some have argued was used to break into Gov. Sarah Palin's e-mail earlier this week.

Google Inc.'s Gmail, Microsoft Corp.'s Windows Live Hotmail and Yahoo Inc.'s Mail all rely on automated password-reset mechanisms that can be abused by anyone who knows the username associated with an account and an answer to a single security question, according to quick tests run by Computerworld.
(from Computer World)

Defending instant messaging
September 20, 2008

"Instant messaging is a very successful means for the bad guys to get their software onto your computer...If a virus infects your friend's computer's instant messaging program then it can "type" anything into the chat windows and it will look like your friend said it. It can provide a link for you to click that may lead you to malicious software."

If you get sent a link to a Web site, verify with your friend that *they* really sent the link. This isn't a perfect defense, as the malware may respond rather than your friend, but it's better than blindly trusting. For users of Windows Live Messenger, he also suggests a configuration change that will prevent the program from downloading many types of malicious software.
(from CNET)

Adobe slates patch for Flash clipboard poisoning attacks
September 22, 2008

Adobe Systems Inc. last week said it will soon quash a bug in Flash that has been used for more than a month by attackers to poison Macintosh and Windows users' clipboards with URLs to malicious sites.

In August, security researchers reported malicious scripts in Flash-based ads on legitimate sites. The scripts abused the "setClipboard" command in Flash to repeatedly infect users' clipboards with URLs pushing fake security software. The scammers hoped that some users would paste the URL into their browsers' address bars and would be duped into purchasing the bogus program once at the phony software site.
(from Computer World)

Study: Vast number of cyber attacks 'Made in the USA'
September 23, 2008

When it comes to cybercrime, Eastern Europe, China, and Brazil may get the lion's share of press attention, but a new study shows a vast proportion of

attacks come from computers in the United States.

Security firm SecureWorks has counted 20.6 million attacks against its customers that originated inside US borders so far this year. China ranked No. 2 on the list with 7.7 million, and Brazil and South Korea came in third and fourth, with 166,987 and 162,298 respectively. The study, which was released Monday, is a strong indication that there's no shortage of compromised computers on US soil.
(from The Register)

Firms ignoring risk of security breaches
September 24, 2008

A new survey from business services firm Logica has found a remarkable lack of awareness about how to manage data and respond to the risks of security weaknesses in enterprise systems.

"With some organisations failing to disclose security breaches, this complacent attitude not only increases the likelihood of financial and reputational consequences, but highlights inadequate security policies and protocols at UK organisations."
(from Vnunet)

Behind the scenes of online fraud
September 25, 2008

Online fraudsters are coming up with more types of dangerous attacks and more sophisticated methods, says Uri Rivner, head of new technologies for RSA Consumer Solutions, which is owned by EMC.

Fraudsters aren't just targeting bank customers. They are also luring victims off social networks, where they harvest sensitive private information, and online gaming sites, where they steal accomplished avatars and accounts and sell them for money, Rivner says.
(from CNET)

Experts warn of new PDF attacks
September 26, 2008

Security organisations are warning users to be vigilant following the discovery of a new crop of tools for exploited PDF flaws.

US-Cert recommends that users protect against the attacks by avoiding untrusted or unsolicited downloads and email attachments.

(from Vnunet)

Microsoft, Washington state sue over 'scareware' pop-up ads
September 29, 2008

Microsoft and the Attorney General's office in Washington state said on Monday they have filed a handful of lawsuits over pop-up ads that scare consumers into paying for software that supposedly fixes critical errors on a PC.

Microsoft filed five new lawsuits and amended two previous complaints against SMP Soft and Registry Update, all relating to programs that allegedly falsely alert consumers to problems on their computers and offer to sell software fixes. The programs listed include Scan & Repair, Antivirus 2009, MalwareCore, WinDefenderXPDefender.com and WinSpywareProtect. Most of the defendants are listed as "John Doe" because investigators do not yet know the identities of the people behind the programs.

(from CNET)

Nasty web bug descends on world's most popular sites
September 30, 2008

Underscoring the severity of an exotic form of website bug, security researchers from Princeton University have cataloged four cross-site request forgeries in some of the world's most popular sites.

The most serious vulnerability by far was in the website of global financial services company ING Direct. The flaw could have allowed an attacker to transfer funds out of a user's account, or to create additional accounts of behalf of a victim, according to this

post from *Freedom to Tinker* blogger Bill Zeller.
(from The Register)

**FOR FURTHER
INFORMATION,
PLEASE CONTACT**

Tel: (852) 8105 6060
Fax: (852) 8105 9760
e-mail: hkcert@hkcert.org
Web Site: <http://www.hkcert.org>

Hong Kong Computer Emergency Response
Team Coordination Centre