

Contents

Contents.....	1
Police Phishing.....	1
HSBC Security	1
Cuebot Exploits MS06-040.....	2
“Experience Windows Vista”: Patch Treadmill Started	2
Two “Patch T-days” in August	2
Backlog of 175 Zero-Day Vulnerabilities	2
Centrino Performance	3
Stupid Security Awards	3
Crime and Technology: Humour.....	3

Police Phishing

Sophisticated criminals have made an exact copy of the Interpol website, at interpolglobal.com. The site was used to create an aura of trust in dealings with victims; the site is now inactive.

The whois information gave the strange address: “Interpol, 152 melony street, london Beijing, GB”, and a Hotmail email address.

More information:

http://www.theregister.com/2006/07/31/scammers_create_interpol_mirror/

HSBC Security

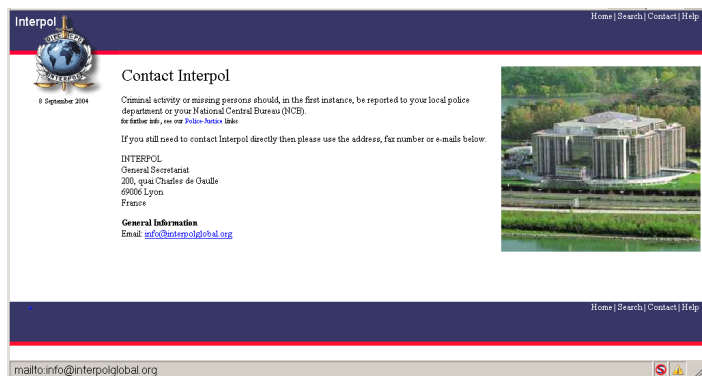
Researchers at Cardiff University claim to have found a flaw in the UK version of HSBC’s online banking system that put “millions” of online accounts at risk for at least two years. However, the sketchy details provided in the [Guardian](#) indicated that the attacker would need a keylogger installed on the victim’s machine. Bruce Schneier [commented](#), “If this is the biggest flaw in HSBC's login authentication system, I think they're doing pretty good.”

HSBC has confirmed that its Hong Kong online banking system does not have the same flaw.

More information:

<http://technology.scmp.com/techmain/ZZZ5JW48KQE.html>

<http://www.schneier.com/crypto-gram-0608.html#10>



<http://technology.guardian.co.uk/news/story/0,,1841016,00.html>

http://www.theregister.com/2006/08/10/flaw_hsbcb/

Cuebot Exploits MS06-040

Microsoft's "Patch Tuesday" this month featured a bunch of critical updates, and, very shortly, two new variants in the Cuebot family were distributed to exploit vulnerability MS06-040.

More information:

<http://www.sophos.com/security/analyses/w32cuebotl.html>

<http://www.sophos.com/security/analyses/w32cuebotm.html>

<http://www.microsoft.com/technet/security/bulletin/MS06-040.msp>

<http://www.dhs.gov/dhspublic/display?content=5789>

<http://www.f-secure.com/weblog/archives/archive-082006.html#00000944>

<http://www.f-secure.com/weblog/archives/archive-082006.html#00000946>

http://www.theregister.com/2006/08/14/cuebot_worm_targets_ms_vuln/

"Experience Windows Vista": Patch Treadmill Started

Beta-testers of Microsoft's upcoming operating system, Windows Vista, can now enjoy a true experience of the future of computing. Microsoft's "Patch Tuesday" this month included two critical patches affecting Windows Vista Beta 2.

More information:

<http://www.microsoft.com/technet/security/Bulletin/MS06-042.msp>

<http://www.microsoft.com/technet/security/Bulletin/MS06-051.msp>

http://www.theregister.com/2006/08/18/vista_security_update/

Two "Patch T-days" in August

MS06-042, released on Tuesday, August 8th, was found to cause Internet Explorer to crash. Worse, security researchers at eEye found it was an exploitable buffer overflow. eEye chose to publish an advisory about the vulnerability on August 22nd, two days before Microsoft had their fix for their fix ready.

Microsoft and eEye are now engaged in a war of words over responsible disclosure, and protection of users.

More information:

<http://research.eeye.com/html/alerts/AL20060822.html>

<http://www.microsoft.com/technet/security/bulletin/ms06-042.msp>

<http://www.microsoft.com/technet/security/advisory/923762.msp>

http://www.theregister.com/2006/08/24/microsoft_flaw_update/

Backlog of 175 Zero-Day Vulnerabilities

NGSSoftware has a database of 175 unfixed vulnerabilities in software products from Oracle, IBM, HP, Microsoft, Openbase, Real, Sybase, Ingres, Veritas, Computer Associates and Sun.

The security consultancy is working with the UK's National Infrastructure Security Co-ordination Centre (NISCC) on the issues.

More information:

http://www.theregister.com/2006/08/24/0-day_manace/

Centrino Performance

Microsoft is not the only company having trouble with their security updates this month. Intel released new, massive, 129MB, Centrino device drivers to deal with vulnerabilities. However, the drivers included a memory leak that caused performance problems.

Intel is aware of the problem and is working on a revised fix.

More information:

<http://www.f-secure.com/weblog/archives/archive-082006.html#00000954>

http://www.theregister.com/2006/08/24/intel_centrino_update_glitch/

<http://isc.sans.org/diary.php?date=2006-08-24>

Stupid Security Awards

Privacy International is accepting nominations for the World's most stupid security measures.

Nominations can be sent to stupidsecurity@privacy.org.

More information:

<http://www.privacyinternational.org/ssa2003winners>

http://www.theregister.com/2006/08/22/stupid_security_awards/

Crime and Technology: Humour

<http://www.dilbert.com/comics/dilbert/archive/dilbert-20060830.html>



Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2870 8550 Fax: 2870 8563
E-mail: info@yuik.com.hk
<http://www.yuik.com.hk/>

<http://www.yuikee.com.hk/>

- Security Software Support & Distribution
- Anti-Virus
- Anti-Spam
- Encryption

E-Learning

- Content & Curriculum Development
- Training

Security

*Your
Peace of Mind
Is Our
Commitment*

- Information Security Consultancy
- Alert Services & Web Monitoring
- Ethics, Safety & Security

Education

- Project Development & Management
- Educational Software Distribution

<http://education.yuikee.com.hk/>