
OSSIR
Groupe Paris
Réunion du 7 avril 2009



Revue des dernières vulnérabilités



Nicolas RUFF
EADS-IW
nicolas.ruff (à) eads.net

Avis Microsoft (1/5)

■ Correctifs de Mars 2009

- Avec [*exploitability index*]
- **MS09-006 Failles dans le décodage EMF/WMF [3/2/3]**
 - Affecte: Windows (toutes versions supportées)
 - Exploit:
 - Fichier EMF ou WMF malformé
 - Décodage en mode noyau (GDI / win32k.sys)
 - Crédit:
 - Helmut Buhler
 - Thomas Garnier / SkyRecon

Avis Microsoft (2/5)

- **MS09-007 Spoofing SCHANNEL [2]**
 - **Affecte: Windows (toutes versions supportées)**
 - **Exploit:**
 - **Authentification par certificat possible, si la partie publique d'un certificat client a été obtenue**
 - **N'affecte que l'authentification avec des comptes locaux**
 - **<http://blogs.technet.com/srd/archive/2009/03/10/assessing-the-risk-of-the-schannel-dll-vulnerability-ms09-007.aspx>**
 - **Crédit: état du Rio Grande do Sul (brésil)**

Avis Microsoft (3/5)

- **MS09-008 Spoofing WINS (x1) et DNS (x3) [2/2/2/2]**
 - **Affecte: Windows (toutes versions serveur supportées)**
 - **Exploit:**
 - Possibilité de *spoof*er une réponse DNS (CVE-2009-0233)
 - Fuite d'information sur les *Transaction ID* par des requêtes particulières (CVE-2009-0234)
 - Enregistrement des noms WPAD/ISATAP (WINS & DNS)
 - **<http://blogs.technet.com/srd/archive/2009/03/13/ms09-008-dns-and-wins-server-security-update-in-more-detail.aspx>**
 - Les réponses RR ne sont jamais mises en cache, ce qui permet de nombreux essais
 - Ajoute les clés "GlobalQueryBlockList" et "QueryBlockList"
 - Ne marche pas si le système a déjà été compromis
 - http://blogs.eweek.com/cheap_hack/content/border_security/ms09-008_patch_ineffective_on_exploited_systems_claims_ncircle.html
 - **Crédit:**
 - Kevin Day
 - Dave Dagon / Georgia Tech

Avis Microsoft (4/5)

■ A noter également

- Mises à jour WSUS
 - <http://support.microsoft.com/kb/894199>
- Mises à jour "non sécurité"
 - <http://technet.microsoft.com/en-us/wsus/bb466214.aspx>
- Mises à jour facultatives sur Windows Update
 - PowerShell 1.0
 - Windows Live

■ Advisories

- 953839 "Kill Bits"
 - "Aurigma Image Uploader"
 - "HP Instant Support"
- 969136 "0day" affectant PowerPoint
 - Affecte: versions antérieures à Office 2007 / 2008 pour Mac
 - <http://blogs.technet.com/srd/archive/2009/04/02/investigating-the-new-powerpoint-issue.aspx>

Avis Microsoft (5/5)

■ Prévisions pour Avril 2009

- Non disponible pour le moment

■ Révisions

- MS08-032
 - Version 1.1: Windows 2008 "Core" n'est pas affecté, mais se voit offrir le correctif
- MS08-040
 - Version 1.9: correction du nom "ADMT" en "ADS"
- MS08-052
 - Version 4.0: nouveau correctif pour Windows XP SP3 et Windows 2003 SP2 (si problème d'installation)
- MS09-004
 - Version 1.2: correction du nom "ADMT" en "ADS"
- MS09-008
 - Version 1.1: clarification sur les systèmes affectés

Infos Microsoft (1/3)

■ Sorties logicielles

- **Internet Explorer 8 en version finale**
 - <http://www.microsoft.com/windows/internet-explorer/worldwide-sites.aspx>
- **La bonne nouvelle: vous pouvez gagner un "finger skate" ☺**
 - <http://www.microsoft.com/france/windows/products/winfamily/ie/ie8/jeu-concours.aspx>
- **Et l'exploitation par injection de bibliothèques .NET ne fonctionne plus**
 - <http://blogs.technet.com/srd/archive/2009/03/23/released-build-of-internet-explorer-8-blocks-dowd-sotirov-aslr-dep-net-bypass.aspx>
- **Beta & RC**
 - Windows Vista / Windows 2008 SP2 en RC
 - SilverLight 3 Beta
- **!exploitable pour WinDbg**
 - <http://msecdbg.codeplex.com/>
 - <http://www.securityfocus.com/brief/928>

Infos Microsoft (1/3)

■ Autre

- **Windows XP en fin de vie**
 - Plus de support à partir du 14 avril 2009
 - Support des correctifs de sécurité jusqu'au 8 avril 2014

- **Microsoft ouvre les 2CENTER**
 - *Cybercrime Centres of Excellence Network for Training, Research and Education*
 - Centre de formation pour les forces de l'ordre
 - Prévu pour 2010 à l'université de Troyes (UTT)
 - <http://www.microsoft.com/Presspass/press/2009/mar09/03-10CybercrimeCentresPR.msp>

Infos Microsoft (2/3)

- **SkyWing rejoint Microsoft**
 - **Encore un contributeur du projet Metasploit**
 - <http://www.threatpost.com/blogs/ken-skywing-johnson-joins-microsoft-security-team>
- **La "faille" GpFont::SetData() non exploitable grâce à /GS**
 - <http://bl4cksecurity.blogspot.com/2009/03/microsoft-gdiplus-emf-gpfontsetdata.html>
 - **Un simple "off by one" (corrigé dans Vista)**
 - <http://blogs.technet.com/srd/archive/2009/03/26/new-emf-gdiplus-dll-crash-not-exploitable-for-code-execution.aspx>
- **Détecter les "heap spray" par émulation de code**
 - <http://research.microsoft.com/en-us/projects/nozzle/>

Infos Microsoft (3/3)

■ Windows Seven

- La RC repoussée à fin mai 2009
 - <http://www.guwiv.com/portal/blogs/news/archive/2009/03/16/exclusif-windows-7-release-candidate-finalement-disponible-fin-mai-2009.aspx>

Infos Réseau

- **Cisco nous gête !**
 - **Cisco IOS cTCP Denial of Service Vulnerability**
 - <http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml>
 - "This vulnerability was found during the resolution of a technical support service request."
 - **Cisco IOS Software WebVPN and SSLVPN Vulnerabilities**
 - <http://www.cisco.com/warp/public/707/cisco-sa-20090325-webvpn.shtml>
 - "These vulnerabilities were discovered when handling customer support calls."
 - **Cisco IOS Software Mobile IP and Mobile IPv6 Vulnerabilities**
 - <http://www.cisco.com/warp/public/707/cisco-sa-20090325-mobileip.shtml>
 - "This vulnerability was reported to Cisco by a customer."
 - **Cisco IOS Software Secure Copy Privilege Escalation Vulnerability**
 - <http://www.cisco.com/warp/public/707/cisco-sa-20090325-scp.shtml>
 - "This vulnerability was reported to Cisco by Kevin Graham."

Infos Réseau

■ Cisco nous gêne ! (suite)

- **Cisco IOS Software Multiple Features Crafted TCP Sequence Vulnerability**
 - <http://www.cisco.com/warp/public/707/cisco-sa-20090325-tcp.shtml>
 - "This vulnerability was found by Cisco internal testing."
- **Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability**
 - <http://www.cisco.com/warp/public/707/cisco-sa-20090325-sip.shtml>
 - "This vulnerability was discovered during handling of customer service requests."
- **Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability**
 - <http://www.cisco.com/warp/public/707/cisco-sa-20090325-udp.shtml>
 - "This vulnerability was discovered by Cisco during routine internal testing."
- **Cisco IOS Software Multiple Features IP Sockets Vulnerability**
 - <http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml>
 - "This vulnerability was discovered by Cisco when performing internal vulnerability testing. We would also like to thank Jens Link, freelance consultant, for also reporting this vulnerability to us."

■ Faut-il patcher ses routeurs ?

- <http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=216200419>

Infos Réseau

- **Cisco va effectivement vendre des serveurs (!)**
 - *Project California*
 - Système d'exploitation RedHat 5.3
 - <http://www.itrmanager.com/articles/88789/cisco-entre-marche-serveurs.html>

- **Cloud Computing**
 - La solution Open Source de Sun
 - <http://www.sun.com/solutions/cloudcomputing/index.jsp>

- **Faille dans CheckPoint FW-1**
 - Affecte: module "PKI Web Service"
 - Exploit:
 - <http://seclists.org/bugtraq/2009/Mar/0261.html>
 - 4 ans avant d'être publiée
 - Et pas de patch ...

■ Actualité

- **Première version de NFTABLES (remplaçant IPTABLES)**
 - <http://lwn.net/Articles/324251/>
- **OpenSSL 2x plus rapide sur noyau 2.6.29**
 - **Encore une optimisation ? ☺**
 - http://www.phoronix.com/scan.php?page=article&item=linux_2629_benchmark&num=4
- **GreenSQL: le proxy SQL**
 - <http://www.greensql.net/>

Infos Unix

■ Failles

- **Failles (non critiques) dans OpenSSL**
 - Affecte: OpenSSL < 0.9.8k
 - Exploit: DoS (x2) + signature incorrecte reconnue comme valide
 - http://www.openssl.org/news/secadv_20090325.txt
- **Faille dans FreeBSD**
 - Affecte : FreeBSD 7.0 et 7.1
 - Exploit : élévation de privilèges locale via un *per-process timer*
 - <http://security.freebsd.org/advisories/FreeBSD-SA-09:06.ktimer.asc>
- **Failles dans mod_security**
 - Affecte : mod_security < 2.5.9
 - Exploit : DoS
 - http://sourceforge.net/project/shownotes.php?release_id=667542&group_id=68846

Infos Unix

- **Faille dans LittleCMS (*Color Management System*)**
 - Affecte: tout produit basé sur LittleCMS
 - OpenJDK, Firefox, GIMP, ...
 - Exploit: fichier JPEG avec un profil ICC malformé
 - <http://scary.beasts.org/security/CESA-2009-003.html>
- **Faille dans DNSSEC sur BIND**
 - Affecte : BIND < 9.4.3-02, 9.5.1-P2
 - Exploit : algorithmes "inconnus" vs. *DNSSEC Lookaside Validation*
- **Faille dans cURL**
 - Affecte: cURL < 7.19.4
 - Exploit: scp:// <whatever> ; <command>
- **Faille Moodle**
 - Affecte: Moodle < 1.8.9 et < 1.9.5
 - Exploit: faille issue du *backend* Latex ☺

Failles

■ Principales applications

- **Acrobat < 9.1, 8.1.4 et 7.1.1**
 - **Faille "JBIG2"**
 - **Attention il y a eu plusieurs failles liées au support JBIG2 corrigées (!)**
 - **Et la faille "surprise" getIcon()**
 - <http://www.zerodayinitiative.com/advisories/ZDI-09-014/>
- **Firefox < 3.0.8**
 - **Faille dans le parser XML**
 - **Publiée en "0day" sur la liste "full disclosure"**
 - **Publique et non patchée pendant au moins une semaine**
- **ThunderBird < 2.0.0.21**
- **iTunes < 8.1**
 - **Faille dans le support du DAAP**
 - **Faille dans le support des baladodiffusions (*podcast*)**
 - <http://support.apple.com/kb/HT3487>

Failles

- **Java < 1.6.13 et < 1.5.18**
 - **Avec des vrais failles de sécurité**
 - <http://labs.odefense.com/intelligence/vulnerabilities/display.php?id=777>
 - <http://labs.odefense.com/intelligence/vulnerabilities/display.php?id=778>
 - <http://labs.odefense.com/intelligence/vulnerabilities/display.php?id=779>
 - <http://labs.odefense.com/intelligence/vulnerabilities/display.php?id=780>
 - <http://labs.odefense.com/intelligence/vulnerabilities/display.php?id=781>
 - **"Preuves de concept" disponibles dans la nature**
- **VMWare (failles multiples)**
 - **Affecte : toutes versions**
 - **Exploit : évasion invité vers hôte, DoS de l'hôte, etc.**
 - <http://lists.vmware.com/pipermail/security-announce/2009/000054.html>
 - **"Preuve de concept" disponible**
 - <http://expertmiami.blogspot.com/2009/04/vmware-escape.html>

Failles

- **"0day" dans Mac OS X**
 - Affecte : Mac OS X 10.4 et 10.5
 - Exploit : élévation de privilèges locale (x5)
 - <http://www.informationweek.com/news/hardware/mac/showArticle.jhtml?articleID=216401181>
 - et ... <http://www.milw0rm.com/>
- **Winamp < 5.551**
- **FileZilla Server < 0.9.31**
 - Bogue dans le support SSL

Failles

- **Faille dans de nombreux produits Symantec ...**
 - ... orientés "messagerie"
 - En cause: traitement des fichiers WordPerfect par le module tiers "Autonomy KeyView"
 - <http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=774>
 - <http://securityresponse.symantec.com/avcenter/security/Content/2009.03.17a.html>
- **Affecte également Lotus Notes**
 - Le même composant est impacté : wp6sr.dll
- **Faille (locale) dans Symantec PCAnywhere**
 - Affecte : PCAnywhere <= 12.5
 - Exploit : Elévation de privilèges locale via un fichier malformé
 - *Format string* (!)
 - <http://securityresponse.symantec.com/avcenter/security/Content/2009.03.17.html>

Malwares et spam

■ Détecter Conficker sur son réseau

- Le code
 - <http://iv.cs.uni-bonn.de/wg/cs/applications/containing-conficker/>
- Utilisation dans Nessus
 - <http://www.nessus.org/plugins/index.php?view=single&id=36036>
- Utilisation dans Nmap
 - <http://www.skullsecurity.org/blog/?p=209>
- A voir aussi
 - http://www.confickerworkinggroup.org/infection_test/cfeyechart.html

■ <http://trafficonverter.net/> éteint

- Un site de "rogue antivirus" notoire
- Remarque: à l'origine du nom "conficker"

Malwares et spam

- **Un problème avec l'antivirus Symantec qui dégénère**
 - <http://isc.sans.org/diary.html?storyid=5992>
 - Etape #1: une mise à jour non signée ("PIFTS.EXE") est poussée par erreur et provoque des dysfonctionnements
 - Etape #2: tous les internautes qui cherchent "PIFTS.EXE" arrivent sur des sites malveillants (SEO malveillant)
 - Très mauvaise gestion de crise chez Symantec
 - <http://www.zdnet.fr/actualites/internet/0,39020774,39387713,00.htm>

- **Il n'y a pas de monopole de la communication "étrange"**
 - http://www.symantec.com/region/fr/norton_heroes/index.html

- **Le futur du e-banking ?**
 - Un PC dans un Token USB !
 - <http://www.zurich.ibm.com/ztic/>

Failles 2.0

- **Un botnet sur modem ADSL trouvé dans la nature ...**
 - **Point d'entrée : interface d'administration exposée et login trivial**
 - <http://dronebl.org/blog/8>
 - <http://www.adam.com.au/bogaurd/PSYBOT.pdf>

- **Un Trojan ... dans un GAB !**
 - <http://www.itwire.com/content/view/23898/53/>

- **Un schéma d'extorsion plutôt original**
 - **Les criminels demandaient des photos de nu !**
 - http://www.myfoxorlando.com/dpp/news/032709FBI_looking_for_cyber_criminal_victims

Failles 2.0

■ Abus des proxies transparents

- Les proxies transparents basent leurs décisions sur l'entête "Host:" plutôt que sur l'adresse IP
- Ceci permet de violer la *Same Origin Policy* à travers les plugins capables de forger cet entête
 - Une liste potentiellement assez longue ...
 - <http://www.kb.cert.org/vuls/id/435052>

■ Le *top 10* des nouvelles attaques Web en 2008

- <http://jeremiahgrossman.blogspot.com/2009/02/top-ten-web-hacking-techniques-of-2008.html>

Actualité (France)

- **Microsoft et Google rejoignent le "passeport pour l'économie numérique"**
 - <http://www.econumerique.pme.gouv.fr/PMEWeb/>

- **91 projets retenus dans les "pôles de compétitivité"**
 - **Dont 20 dans le pôle SYSTEM@TIC**
 - <http://www.bulletins-electroniques.com/actualites/58313.htm>

- **Vers une certification des sociétés d'intelligence économique ?**
 - <http://fr.securityvibes.com/etat-entreprise-espionnage-industriel-article-1009.html>

- **Un téléphone portable sécurisé pour les VIP français ?**
 - <http://fr.news.yahoo.com/4/20090403/tts-france-securite-thales-ca02f96.html>

- **EDF aurait piraté GreenPeace**
 - <http://www.mediapart.fr/journal/france/310309/edf-aurait-fait-espionner-greenpeace>

- **Pirate ou consultant, il faut choisir**
 - http://www.laprovence.com/print/2009/04/02/article_775855.html

Actualité (France)

■ HADOPI, suite

- Round #1: Jacques Attali vs. HADOPI
 - <http://blogs.lexpress.fr/attali/2009/03/une-loi-scandaleuse-et-ridicul.php>
- Round #2: le SNEP lui demande s'il voudrait voir ses livres téléchargés
- Round #3: les livres sont librement téléchargeables au format PDF !
 - <http://www.zataz.com/news/18716/jacques-attali--livre--telechargement.html>
- Et sinon ...
 - Usurper une IP, c'est facile
 - <http://www.pcinpact.com/actu/news/49642-suspension-internet-abonnement-ip-constat.htm>

Actualité (France)

- **"Fabriquer" une IP, c'est facile (!)**
 - <http://www.numerama.com/magazine/12264-La-Quadrature-du-Net-accusee-par-le-cabinet-d-Albanel-de-fabriquer-des-IP.html>
- **Le parlement européen ne veut décidément pas de la coupure**
 - <http://www.itrmanager.com/articles/89283/parlement-europeen-redit-coupure-acces-internet.html>
- **Le site "J'aime les artistes" piraté suite à la déclaration suivante de la ministre: "ils peuvent toujours attaquer, le site est super blindé"**
 - <http://www.numerama.com/magazine/12304-Quand-le-ministere-de-la-Culture-agite-le-chiffon-rouge-les-hackers-chargent.html>
- **Télécharger des artistes qui fraudent le fisc restera possible**
 - <http://www.20minutes.fr/article/317429/Culture-Hadopi-l-Assemblee-vote-un-amendement-Johnny.php>
- **Ceci n'est pas un poisson d'avril ...**
 - <http://www.youtube.com/watch?v=61nwMUhkUJM>

Actualité (France)

- **Ailleurs dans le monde ...**
 - **La Nouvelle-Zélande abandonne l'idée de la coupure Internet**
 - **La "liste noire" des sites filtrés par le gouvernement australien**
 - **http://wikileaks.org/wiki/Australian_government_secret_ACMA_internet_censorship_blacklist%2C_6_Aug_2008**

Actualité (anglo-saxonne)

■ CanSecWest

- **Compromission du code SMM par le cache processeur**
 - Attaque découverte simultanément par Loïc Duflot et Joanna Rutkowska
 - <http://theinvisiblethings.blogspot.com/2009/03/independent-attack-discoveries.html>
- **Ecoute du clavier à distance par:**
 - Le pointage laser des touches (!)
 - Les fuites de masse (!!)
 - http://www.csoonline.com/article/484418/Researchers_Sniff_Keystrokes_from_Thin_Air
- **Outil !exploitable de Microsoft**
 - Cf. actualité Microsoft

Actualité (anglo-saxonne)

■ CanSecWest (suite)

• Concours Pwn2Own

– IE8, Safari et FireFox sont tombés immédiatement

- La faille Safari avait été gardée en réserve pendant 1 an (!)
- Et la technique d'exploitation utilisée contre IE8 ne fonctionne plus dans la version finale ...
 - <http://blogs.technet.com/srd/archive/2009/03/23/released-build-of-internet-explorer-8-blocks-dowd-sotirov-aslr-dep-net-bypass.aspx>

– Revue de presse

- <http://twitter.com/tippingpoint1>
- <http://dvlabs.tippingpoint.com/blog/2009/03/18/pwn2own-2009-day-1---safari-internet-explorer-and-firefox-taken-down-by-four-zero-day-exploits>
- <http://www.securityfocus.com/news/11549>
- <http://www.h-online.com/security/Pwn2Own-2009-Safari-IE-8-and-Firefox-exploited--/news/112889>

Actualité (anglo-saxonne)

■ IBM rachète Sun (?)

- <http://www.itrmanager.com/articles/88888/ibm-discussion-racheter-sun.html>
- http://blogs.spectrum.ieee.org/tech_talk/2009/03/for_ibm_the_allure_of_sun_lies.html
- Quel impact sur Java, MySQL, OpenOffice, etc.
 - <http://www.journaldunet.com/developpeur/expert/37342/si-ibm-achetait-sun---quelle-consequence-pour-le-monde-java.shtml>

■ Un guide de sécurisation MS-SQL

- Notez la référence aux HSM !
 - <http://www.ic3.gov/media/2008/081215.aspx>

■ Matasano sort un produit

- Administration Web de firewalls
 - <http://runplaybook.com>

■ IBM transfère 5000 emplois des USA en Inde

- <http://www.itrmanager.com/articles/89274/ibm-supprimerait-5-000-emplois.html>

Actualité (anglo-saxonne)

■ Une fraude avérée aux machines électorales

- Depuis 2002 ...
- Pas d'éléments techniques complexes ...
- ... mais simplement une faille d'ergonomie dans la GUI
 - <http://www.bradblog.com/?p=7001>

■ La BBC joue aux pirates

- Programme d'origine
 - http://news.bbc.co.uk/1/hi/programmes/click_online/7932816.stm
- Commentaires (nombreux ...)
 - <http://www.sophos.com/blogs/gc/g/2009/03/12/bbc-break-law-botnet-send-spam/>
 - <http://www.smh.com.au/news/technology/security/bbc-cybercrime-probe-backfires/2009/03/13/1236447465056.html>

Actualité (Google)

■ Encore un bogue dans les applications Google

- Cette fois-ci, Google Docs
 - <http://www.01net.com/editorial/405039/google-docs-partage-un-peu-trop-les-documents/>
- L'association EPIC porte plainte (suite à cette faille) !
 - <http://www.zdnet.fr/actualites/internet/0,39020774,39387974,00.htm>
- Et re-Google Docs !
 - <http://www.techcrunch.com/2009/03/26/more-security-loopholes-found-in-google-docs/>

■ Google + General Electric = Smart Grid

- <http://energie.lexpansion.com/articles/Prospective/2009/03/Quand-Google-se-fiance-avec-General-Electric/>
- <http://www.google.org/powermeter/>
- Déjà vulnérable ?
- Ou une opération de com' d'IOActive ?
 - <http://www.cnn.com/2009/TECH/03/20/smartgrid.vulnerability/index.html>

Actualité (Google)

- **Début du Google Summer of Code**

- <http://www.securityfocus.com/brief/934>

- **Nouvelle fonction dans GMail : "undo send" (!)**

- En Beta bien sûr 😊

- <http://gmailblog.blogspot.com/2009/03/new-in-labs-undo-send.html>

Actualité

■ Analyse de l'opération "GhostNet"

- **Attaques ciblées du gouvernement chinois contre des ONG**
 - <http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.html>
- **(Miroirs)**
 - <http://www.f-secure.com/weblog/archives/ghostnet.pdf>
 - <http://www.f-secure.com/weblog/archives/UCAM-CL-TR-746.pdf>

■ Etude Verizon

- **500 cas étudiés**
- **70% des intrusions mettent plus d'un an à être détectées**
 - <http://www.verizonbusiness.com/resources/security/databreachreport.pdf>

■ Etude KPMG

- **La fraude interne a triplé entre 2007 et 2008**
 - <http://www.datanews.be/fr/news/90-55-23205/la-crise-pousserait-les-informaticiens-dans-la-criminalite.html>

- **Open Software Assurance Maturity Model**
 - <http://www.opensamm.org/>

- **La cour constitutionnelle allemande déclare les machines à voter illégales**
 - <http://www.bundesverfassungsgericht.de/en/press/bvg09-019en.html>

Actualité

- **Les centres de paiement Heartland et WorldPay punis par Visa**
 - Leur agrément PCI/DSS leur a été retiré suite à l'intrusion dont ils ont été victimes
 - <http://www.scmagazineus.com/Visa-Heartland-RBS-WorldPay-no-longer-PCI-compliant/article/128762/>

- **L'expert judiciaire de l'affaire "Pirate Bay" piraté !**
 - En cause: ses liens avec Warner
 - <http://torrentfreak.com/hackers-go-after-pirate-bay-investigator-090327/>

- **Un nouveau moteur de recherche sémantique**
 - Lancement en mai 2009
 - <http://www.wolframalpha.com/>

- **Le projet européen Humabio**
 - Biométrie à base de données corporelles
 - (Ondes cérébrales et rythme cardiaque)
 - <http://www.atelier.fr/securite/10/09022009/biometrie-capteur-securite-identite-cerveau-coeur-37806-.html>

- L'algorithme de génération des *vouchers* iTunes craqués par des Chinois
 - Ca va coûter cher à Apple ...
 - <http://www.trustedreviews.com/mp3/news/2009/03/10/iTunes-Voucher-Codes-Hacked/p1>
 - Mais que fait HADOPI ?

- Quoi de plus simple que `strlen()` ?
 - <http://sources.redhat.com/cgi-bin/cvsweb.cgi/libc/string/strlen.c?rev=1.1.2.1&content-type=text/x-cvsweb-markup&cvsroot=glibc>

Questions / réponses

- Questions / réponses
- Prochaine réunion
 - Mardi 12 mai 2009
- N'hésitez pas à proposer des sujets et des salles