
OSSIR
Groupe Paris
Réunion du 12 janvier 2010



Revue des dernières vulnérabilités



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

Avis Microsoft (1/8)

■ Correctif de Décembre 2009

- 6 bulletins, 12 failles
- Avec [*exploitability index*]
- Voir aussi:
 - <http://blogs.technet.com/srd/archive/2009/12/08/assessing-the-risk-of-the-december-security-bulletins.aspx>
- MS09-069 Faille dans ISAKMP / LSASS [3]
 - Affecte: Windows 2000 / XP / 2003
 - Exploit: déni de service par épuisement de ressources
 - L'attaquant doit établir un tunnel IPSEC préalablement
 - Crédit: n/d
- MS09-070 Faille dans ADFS [3,1]
 - Affecte: Windows 2003 R2, Windows 2008
 - Exploit:
 - *Spoofing* du SSO Web (si l'attaquant a accès au navigateur d'un utilisateur préalablement authentifié)
 - Exécution de code à distance via une requête HTTP malformée (et authentifiée)
 - Crédit: n/d

Avis Microsoft (2/8)

- **MS09-071 Faille dans IAS [2,3]**
 - **Affecte:** Windows (toutes versions supportées sauf Seven / 2008 R2)
 - **Exploit:** contournement de l'authentification, corruption mémoire
 - Seulement si l'authentification PEAP + MS-CHAPv2 est utilisée
 - **Crédit:** n/d

- **MS09-072 Patch cumulatif pour IE [1,1,1,1]**
 - **Affecte:** IE (toutes versions supportées)
 - **Exploit:**
 - <http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=833>
 - <http://www.zerodayinitiative.com/advisories/ZDI-09-086/>
 - <http://www.zerodayinitiative.com/advisories/ZDI-09-087/>
 - **Crédit:**
 - Ryan Smith / Verisign IDefense Labs
 - Sam Thomas / eshu.co.uk + TippingPoint+ZDI
 - team509 / Verisign IDefense Labs
 - Anonymous / TippingPoint+ZDI (x2)

Avis Microsoft (3/8)

- **MS09-073 Faille dans un convertisseur de texte [2]**
 - **Affecte:**
 - Windows 2000 / XP / 2003 (Wordpad)
 - Office XP / 2003
 - Works 8.5
 - **Exploit: exécution de code à l'ouverture d'un document Word 97**
 - <http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=834>
 - **Crédit: Sean Larsson & Jun Mao / VeriSign iDefense Labs**

- **MS09-074 Faille dans Microsoft Project [2]**
 - **Affecte: Microsoft Project 2000 / XP / 2003**
 - **Exploit: exécution de code à l'ouverture d'un document Project malformé (.mpp)**
 - **Crédit: Bing Liu / Fortinet**

Avis Microsoft (4/8)

■ A noter également

- **ASP ne gère pas correctement les doubles extensions de type ".asp;.jpg"**
 - <http://soroush.secproject.com/downloadable/iis-semicolon-report.pdf>
 - N'affecte pas ASP.NET
- **Réponse de Microsoft:**
 - <http://blogs.technet.com/msrc/archive/2009/12/27/new-reports-of-a-vulnerability-in-iis.aspx>
 - <http://blogs.technet.com/msrc/archive/2009/12/29/results-of-investigation-into-holiday-iis-claim.aspx>

■ Prévisions pour Janvier 2010

- **1 bulletin critique pour Windows 2000**
 - Impact faible sur les autres plateformes

Avis Microsoft (5/8)

■ Advisories

- **954157 "Security Enhancements for the Indeo Codec"**
 - **V1.0: il est recommandé de désinstaller complètement le codec Indeo32**
 - **Il existe des faille(s) découvertes par**
 - **Paul Byrne / NGS Software**
 - **Anonymous / TippingPoint+ZDI**
 - **Bing Liu / Fortinet**
 - **VeriSign iDefense Labs**
 - **Dave Lenoe / Adobe**

Avis Microsoft (6/8)

- **973811 "Extended Protection for Authentication"**
 - **V1.2: cette option est désormais supportée par les composants**
 - **Windows HTTP Services**
 - **HTTP Protocol Stack (http.sys)**
 - **IIS**
 - <http://support.microsoft.com/kb/973917>
 - **Attention aux effets de bord !**
 - <http://support.microsoft.com/kb/2009746>
 - **Basé sur RFC 5006**
 - **Voir aussi:**
 - <http://blogs.technet.com/srd/archive/2009/12/08/extended-protection-for-authentication.aspx>

Avis Microsoft (7/8)

- **974926 "Credential Relaying Attacks on Integrated Windows Authentication"**
 - **V1.0: revue des protections fournies par Microsoft**
- **977981 Faille dans IE6/IE7 exploitée dans la nature en "0day"**
 - **V2.0: faille corrigée par le bulletin MS09-072**

Avis Microsoft (8/8)

■ Révisions

- **MS08-037**
 - V3.0: nouvelle version du correctif pour Windows 2000 SP4
 - V3.1: corrections typographiques & clarifications
- **MS09-037**
 - V2.1: ajout d'un problème connu (KB973908)
- **MS09-058**
 - V1.1: ajout d'un problème connu (KB971486)
- **MS09-070**
 - V1.1: corrections typographiques & clarifications
- **MS09-071**
 - V1.1: corrections typographiques & clarifications
- **MS09-072**
 - V1.1: corrections typographiques & clarifications
- **MS09-073**
 - V1.1: corrections typographiques & clarifications

Infos Microsoft

■ Sorties logicielles

- Lancement officiel de la plateforme Azure

■ Autre

- **Navigateurs: le principe du *ballot screen* aléatoire entériné**
 - <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/559&format=HTML&aged=0&language=FR&guiLanguage=fr>
 - <http://www.freenews.fr/spip.php?article7489>
 - <http://www.itespresso.fr/internet-explorer-windows-microsoft-et-bruxelles-scellent-un-accord-32877.html>
- **Si vous avez peur de COFEE ...**
 - <http://decafme.org/>
 - **Attention, il vaut mieux utiliser la version *non backdoorée* ☺**
 - <http://www.soldierx.com/news/DECAF-hacked-and-re-enabled-SX>
- **Contournement de SEHOP sous Windows Seven**
 - <http://www.segmentationfault.fr/securite-informatique/bypassing-sehop-on-windows-7/>

- **Un certificat expiré bloque tous les documents Office 2003 protégés par RMS**
 - http://blogs.technet.com/office_sustained_engineering/archive/2009/12/12/cannot-open-office-2003-documents-protected-with-rms-update.aspx

- **Les "God Modes" de Windows Seven**
 - <http://www.developpez.net/forums/d858286/club-professionnels-informatique/actualites/windows-7-cache-plusieurs-godmodes-voici-dautres/>

Infos Réseau

■ Principales failles

- **"Crash" dans toutes les versions de JUNOS par une option TCP malformée**
 - <http://praetorianprefect.com/archives/2010/01/junos-juniper-flaw-exposes-core-routers-to-kernal-crash/>
 - <http://ptresearch.blogspot.com/2010/01/juniper-junos-remote-kernel-crash-flaw.html>
- **Faille exploitable à distance dans F5 BIG-IP**
 - **Affecte:**
 - Application Security Manager (ASM)
 - Protocol Security Manager (PSM)
 - **Exploit:**
 - <http://isc.sans.org/diary.html?storyid=7807>
- **Créer une boucle infinie entre 2 serveurs NTP**
 - **Affecte:** ntpd < 4.2.4p8
 - **Exploit:** <http://www.kb.cert.org/vuls/id/568372>

Infos Réseau

■ Autres infos

- **La zone racine va être signée (DNSSEC)**
 - <http://www.icann.org/en/announcements/announcement-2-09oct08-en.htm>
- **Mais la signature SHA-256 n'est supportée que par BIND 9.6.1**

Infos Unix

■ (Principales) failles

- "Petit problème" avec la fragmentation IP
 - Affecte: noyau Linux 2.6.29+
 - Exploit:
 - <http://git.kernel.org/?p=linux/kernel/git/davem/net-2.6.git;a=commitdiff;h=bbf31bf18d34caa87dd01f08bf713635593697f2>
- PHP < 5.2.12
 - http://www.php.net/releases/5_2_12.php
- SendMail < 8.14.4
 - Principalement des problèmes avec SSL/TLS
 - <http://www.sendmail.org/releases/8.14.4>
- PostgreSQL (toutes versions supportées)
 - <http://www.postgresql.org/docs/current/static/release.html>
 - <http://www.postgresql.org/about/news.1170>

Infos Unix

- **FreeBSD 7 et 8**
 - **Elévation de privilèges locale via ZFS**
 - <http://security.freebsd.org/advisories/FreeBSD-SA-10:03.zfs.asc>
- **Comportement non documenté de FreeBSD**
 - **Evasion de *jail* si *root* utilise la commande *cwd***
 - <http://www.freebsd.org/cgi/query-pr.cgi?pr=142341>
- **Le support NIS sous Debian permet de lire le fichier "shadow"**
 - <http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=560333>
- **Faille dans strtod()**
 - **Affecte: Mac OS X, *BSD, FireFox, ...**
 - <http://isc.sans.org/diary.html?storyid=7942>

Infos Unix

- **phpMyVisites < 2.4**
 - **Module tiers vulnérable à une faille "include"**
 - <http://www.phpmyvisites.us/#infohack>
- **phpCalendar <= 1.1**
 - **Faille "include"**
 - <http://seclists.org/fulldisclosure/2009/Dec/399>
- **Cacti < 0.8.7e**
 - **Injection de commandes *shell* (par un administrateur distant)**
 - <http://archives.neohapsis.com/archives/fulldisclosure/2009-11/0292.html>

■ Autre

- **Interview de Brad Spengler**
 - <http://slo-tech.com/clanki/10001en/>
- **Debian envisage d'utiliser les paquets Ubuntu ☺**
- **Un malware trouvé dans un économiseur d'écran**
 - <http://www.omgubuntu.co.uk/2009/12/malware-found-in-screensaver-for-ubuntu.html>

Failles

■ Principales applications

- **Flash < 10.0.42.34**
 - <http://www.adobe.com/support/security/bulletins/apsb09-19.html>
 - Voir aussi
 - <http://www.zerodayinitiative.com/advisories/ZDI-09-092/>
 - <http://www.zerodayinitiative.com/advisories/ZDI-09-093/>
 - (...)
- **Flash 9 n'est normalement plus supporté**
 - Mais il existe une mise à jour pour les systèmes non compatibles avec Flash 10
 - <http://kb2.adobe.com/cps/406/kb406791.html>
- **Sans oublier Flash Media Server < 3.5.2**
 - <http://www.adobe.com/support/security/bulletins/apsb09-18.html>

Failles

- **Faille dans Acrobat Reader (toutes versions supportées)**
 - Trouvée "dans la nature" dans des attaques ciblées (très bien faites)
 - <http://www.f-secure.com/weblog/archives/00001836.html>
 - Rapidement disponible dans Metasploit
 - <http://twitter.com/hdmoore/statuses/6706530082>
 - Correctif prévu pour le 12 janvier 2010
 - Soit presque 1 mois après !
 - http://blogs.adobe.com/psirt/2009/12/new_adobe_reader_and_acrobat_v.html

Failles

- **La mise à jour sera silencieuse**
 - <http://www.h-online.com/security/news/item/Adobe-to-introduce-silent-updates-for-Reader-896979.html>
- **Il existe une parade**
 - **Les versions récentes (8.1.7 et 9.2) d'Acrobat supportent le blocage sélectif de JavaScript**
 - http://kb2.adobe.com/cps/504/cpsid_50431.html
 - **Il suffit donc de bloquer la fonction DocMedia.newPlayer**
 - http://kb2.adobe.com/cps/532/cpsid_53237.html

Failles

- **ThunderBird < 3.0**
 - En plus la version 3.0 a été fortement inspirée par la gendarmerie française 😊
 - <http://www.clubic.com/actualite-315348-mozilla-thunderbird-gendarmerie.html>
- **WireShark < 1.2.5**
 - <http://www.wireshark.org/security/wnpa-sec-2009-09.html>
- **Winamp < 5.571**
 - http://www.winamp.com/help/Version_History#Winamp_5.571_.28Latest.29

Failles

- **FireFox < 3.5.6**
 - <http://www.mozilla.org/security/known-vulnerabilities/firefox35.html#firefox3.5.6>
 - **Mais cette version a un bogue dans le support des proxies avec authentification NTLM ...**
 - Probablement due au fait qu'un mécanisme anti- "*credential reflection*" a été mis en place !
 - <http://www.mozilla.org/security/announce/2009/mfsa2009-68.html>
 - https://bugzilla.mozilla.org/show_bug.cgi?id=535193
 - **Corrigé dans FireFox 3.5.7**
 - <http://www.mozilla-europe.org/fr/firefox/3.5.7/releasenotes/>

Failles

- **HP OpenView prend cher ...**
 - Suite au rachat de 3Com (donc ZDI) par HP ?
 - Voir TPTI-09-08 ... TPTI-09-14
 - <http://dvlabs.tippingpoint.com/advisory/>
 - Voir ZDI-09-094 ... ZDI-09-098
 - <http://www.zerodayinitiative.com/advisories/>
- **Ruby < 1.9.1-p376**
 - *Heap Overflow* dans le traitement des chaînes de caractères
 - <http://www.ruby-lang.org/en/news/2009/12/07/heap-overflow-in-string>
- **Des nouvelles versions de Metasploit comme s'il en pleuvait ...**
 - 3.3.1, 3.3.2, 3.3.3 ...
 - http://www.metasploit.com/redmine/projects/framework/wiki/Release_Notes_333

Failles

- **Le mois du "0day" s'annonce**
 - <http://www.intevydis.com/blog/?p=109>
 - **Attention à la "faille" MySQL, elle nécessite l'activation YaSSL ...**
- **Contournement de l'authentification sur les routeurs D-Link**
 - **A l'aide du protocole HNAP**
 - http://www.sourcesec.com/Lab/dlink_hnap_captcha.pdf

Failles 2.0

- **32 millions de mots de passe Facebook & MySpace en clair ...**
 - **Perdus par l'application RockYou**
 - <http://www.techcrunch.com/2009/12/14/rockyou-hack-security-myspace-facebook-passwords/>
 - **Et la gestion de crise ne semble pas être leur fort !**

 - **Voir aussi le Hall of Shame:**
 - <http://igigi.baywords.com/>

- **Twitter perd son entrée DNS**
 - **Suite à un piratage de la console d'administration**
 - <http://isc.sans.org/diary.html?storyid=7774>
 - <http://www.zdnet.fr/actualites/internet/0,39020774,39711715,00.htm>

- **Vague d'injections SQL**
 - **132,000 sites compromis par le même outil**
 - <http://www.net-security.org/secworld.php?id=8604>

Failles 2.0

- **Facebook change sa "privacy policy"**
 - Il est désormais possible de rendre des parties de son profil "publiques" ...

- **Le langage FQL permet de lire les données Facebook de n'importe qui**
 - <http://mkdot.net/blogs/slavco/archive/2009/12/29/11338.aspx>

- **Un point de vue intéressant sur la sécurité de Facebook**
 - <http://cert.lexsi.com/weblog/index.php/2010/01/05/352-pourquoi-facebook-a-crucifie-la-securite>

- **Web Application Security Consortium**
 - **Classification des menaces, version 2**
 - <http://projects.webappsec.org/Threat-Classification>

Malwares et spam

- **"Antivirus of the Year (2009)"**
 - Une étude indépendante (?)
 - <http://www.av-comparatives.org/comparativesreviews/main-tests/summary-reports>

- **Le top 10 des botnets (et leurs impacts)**
 - <http://www.net-security.org/secworld.php?id=8599>

- **Le malware Zeus supporte Windows Seven et IPv6**
 - <http://blog.damballa.com/?p=438>

- **Un schéma d'arnaque très bien fait**
 - "Google Adwork"
 - http://news.cnet.com/8301-27080_3-10410831-245.html
 - ... et rentable
 - <http://www.networkworld.com/news/2009/120809-company-sued-by-google-had.html>

- **1 milliard de spams ... les leçons à en tirer**
 - http://www.projecthoneypot.org/1_billionth_spam_message_stats.php

Malwares et spam

- **Un petit malin publie des applications bancaires malveillantes**
 - **Sur Android MarketPlace**
 - <http://www.f-secure.com/weblog/archives/00001852.html>

- **Une campagne d'attaques visant les utilisateurs d'OWA**
 - <http://isc.sans.org/diary.html?storyid=7918>

- **Koobface présente ses vœux à l'industrie de la sécurité**
 - <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>

- **La faille Java "util.calendar" commence à être exploitée "dans la nature"**
 - **Combien de Java < 1.6.11 encore dans la nature ?**
 - <http://isc.sans.org/diary.html?storyid=7879>

- **Le moteur de recherche présent sur "office.microsoft.com" intègre des liens externes malveillants**
 - <http://securitylabs.websense.com/content/Alerts/3519.aspx>

Actualité (France)

- **Une équipe menée par l'INRIA factorise RSA-768**
 - http://www.securite-informatique.gouv.fr/gp_article709.html
 - <http://eprint.iacr.org/2010/006.pdf>

- **SecSip: un pare-feu applicatif pour SIP**
 - <http://secsip.gforge.inria.fr/>

- **Création de nouvelles entités présidées par le chef de l'Etat**
 - Conseil de défense et de sécurité nationale (CDSN)
 - Conseil national du renseignement (CNR)

- **La langue française s'enrichit encore**
 - Avec ordiphone, encre en poudre, etc.
 - <http://www.pcinpact.com/actu/news/54731-vocabulaire-france-informatique-neologisme-commission.htm>

Actualité (France)

- **Un guide de sécurisation à destination des PME**
 - <http://www.hfd.bercy.gouv.fr/guide091207.pdf>
- **Le secrétariat à l'économie numérique va-t-il disparaître ?**
 - <http://www.itespresso.fr/vie-publique-vers-la-disparition-du-secretaire-detat-a-leconomie-numerique-32956.html>
- **"Il faut nationaliser Internet comme les Chinois l'ont fait"**
 - http://www.lepost.fr/article/2009/12/17/1845586_pour-le-depute-ump-jacques-myard-il-faut-nationaliser-internet-comme-les-chinois-l-ont-fait.html
- **Skyrecon StormShield obtient la certification FIPS 140-2 pour son chiffrement de disque**
 - <http://www.skyrecon.com/fr/USB-Peripheriques-Disque-Fichier-Chiffrement>

Actualité (anglo-saxonne)

■ Le gouvernement américain adopte OpenID

- http://www.idmanagement.gov/drilldown.cfm?action=openID_openGOV

■ Le gouvernement australien arrête de filtrer Internet

- Maintenant ce sont les FAI qui vont devoir s'y coller
 - http://www.theregister.co.uk/2009/12/15/australian_censorship_measures/

■ 4500 sites fermés

- ... par effet de bord d'un mail du gouvernement canadien
 - <http://www.monblog.ch/commedansdubeurre/?p=200912301525451>

Actualité (anglo-saxonne)

■ Un concours de *backdoors hardware*

- Avec des résultats intéressants

- <http://spectrum.ieee.org/semiconductors/design/creative-winners-in-hardware-trojan-contest/>

Actualité (anglo-saxonne)

■ TSA FAIL

- <http://boardingarea.com/blogs/viewfromthewing/2009/12/06/the-tsa-puts-their-sensitive-security-screening-procedures-online-for-all-to-see-oops/>

■ Drone FAIL

- Les transmissions descendantes ne sont pas chiffrées
 - <http://online.wsj.com/article/SB126102247889095011.html>
 - <http://www.lepoint.fr/actualites-monde/2009-12-17/irak-afghanistan-les-insurges-interceptent-les-images-video-transmises-par-les/1648/0/406048>

■ La puissance des réseaux sociaux démontrée

- Par une chasse au trésor "grandeur nature"
 - <http://www.bulletins-electroniques.com/actualites/61548.htm>

Actualité (Google)

■ Android 2.0 "jailbreaké"

- <http://alldroid.org/viewtopic.php?f=210&t=567>

■ Droid FAIL

- La même faille que sur iPhone à sa conception 😊
 - <http://www.gizmodo.fr/2010/01/12/une-faille-de-securite-sur-le-droid-permet-dacceder-a-vos-donnees-personnelles.html>

■ Sortie officielle de Chrome pour Linux

- <http://www.google.com/chrome/intl/en/w00t.html>
- ... ainsi que du port BSD 😊
 - <http://marc.info/?l=openbsd-ports-cvs&m=126117522816158&w=2>

■ Google vs. presse française

- <http://www.lavoixdudodo.info/2009/12/08/google-vs-presse-francaise-le-clash-a-bien-eu-lieu/>

■ Google fait peur

- <http://www.generation-nt.com/google-monopole-ministre-allemande-strategie-actualite-940101.html>

Actualité (Google)

■ Eric Schmidt (CEO Google)

- "Si vous voulez effacer vos traces sur Internet, c'est peut-être que vous avez quelque chose à vous reprocher"
 - <http://eco.rue89.com/2009/12/08/le-pdg-de-google-contre-le-droit-a-loubli-sauf-pour-lui-meme-129162>
- **Résultat: la fondation Mozilla recommande d'utiliser Bing !**
 - http://www.lemonde.fr/technologies/article/2009/12/11/des-responsables-de-mozilla-prennent-leurs-distances-avec-google_1279114_651865.html

Actualité (Google)



Actualité (crypto)

■ Les attaques en "*side channel*" progressent

- <http://rdist.root.org/2009/12/30/side-channel-attacks-on-cryptographic-software/>

■ Clés USB sécurisées (certifiées FIPS 140) FAIL

- <http://www.verbatim.com/security/security-update.cfm>
- <http://www.sandisk.com/business-solutions/enterprise/technical-support/security-bulletin-december-2009>
- <http://www.kingston.com/driveupdate/>
- <http://www.kingston.com/flash/DTblackbox.asp>

Actualité

- **La conférence CCC s'impose encore une fois comme une conférence majeure**
 - **A5/1 + GSM complètement cassé**
 - http://events.ccc.de/congress/2009/Fahrplan/attachments/1479_26_C3.Karsten.Nohl.GSM.pdf
 - <http://reflexor.com/trac/a51>
 - **Un pentest qui tourne au drame**
 - <http://events.ccc.de/congress/2009/Fahrplan/events/3596.en.html>
 - **Etc.**

Actualité

■ Qui (n')avait (pas) prévu le bogue de l'an 2010 ?

- **SpamAssassin**

- <http://www.arrfab.net/blog/?p=174>

- **Symantec Endpoint Protection**

- <http://www.symantec.com/connect/forums/official-status-sepm-definitions-stay-31-12-2009-last-updated-04-jan-2010>

- **DShield.org**

- <http://isc.sans.org/diary.html?storyid=7873>

- **Et surtout ... 20 millions de CB allemandes !**

- <http://www.lesechos.fr/info/finance/300401513.htm>

Actualité

■ BackTrack 4 finale

- <http://www.backtrack-linux.org/downloads/>

■ Firefox devient le navigateur le plus utilisé

- <http://www.axiis.org/examples/BrowserMarketShare.html>

■ Le chiffrement de plus en plus souvent contourné ...

- ... par la lecture des données en mémoire
 - http://www.darkreading.com/vulnerability_management/security/attacks/showArticle.jhtml?articleID=222002720
- (PCI/DSS FAIL)

■ Une nouvelle attaque sur Intel TXT

- Via la table ACPI "DMA Remapping"
- Seul 32 bits sont vérifiés sur un registre de configuration 64 bits
 - <http://theinvisiblethings.blogspot.com/2009/12/another-txt-attack.html>

- **L'ENISA produit le manuel du parfait CERT**
 - <http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs>

- **Cloud Security Alliance: le guide en version 2**
 - <http://www.cloudsecurityalliance.org/pr20091217.html>

- **Un cyber-ONU en préparation ?**
 - **Discussions entre russes et américains**
 - http://www.nytimes.com/2009/12/13/science/13cyber.html?_r=4

- **Anti-anti-sec**
 - <http://archives.neohapsis.com/archives/fulldisclosure/2009-12/0489.html>
 - <http://www.anti-sec.com/>

Fun

- **Fabrice Bellard bat le record des décimales de Pi**
 - En utilisant 1 seul PC ...
 - <http://bellard.org/pi/pi2700e9/announce.html>
- **La page d'accueil de la présidence européenne piratée par Mr Bean ☺**
 - <http://www.zdnet.fr/actualites/internet/0,39020774,39711928,00.htm>
- **Cadre photo Kodak FAIL**
 - <http://seattlewireless.net/~casey/?p=13>
- **La base de données des enfants sages a été piratée ☺**
 - <http://precision-blogging.blogspot.com/2009/12/another-leak-worst-so-far.html>
- **Metasploit ajoute le mode AYBABTU**
 - <https://www.metasploit.com/redmine/issues/562>
- **Linus vs. KDB**
 - <http://linuxmafia.com/faq/Kernel/linus-im-a-bastard-speech.html>

Questions / réponses

- Questions / réponses
- Prochaine réunion
 - Mardi 9 février 2010
- N'hésitez pas à proposer des sujets et des salles