OSSIR
Groupe Paris

Réunion du 9 février 2010

Revue des dernières vulnérabilités

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

Avis Microsoft (1/9)

- **Correctif de Janvier 2009**
  - **1 bulletin, 1 faille**
  - **Avec [*exploitability index*]**
  - **MS10-001 Faille dans les polices EOT [2]**
    - **Affecte: Windows (toutes versions supportées)**
      - **N'affecte que Windows 2000 (le code vulnérable n'est jamais appelé sur les autres plateformes)**
      - **La vulnérabilité se situe dans T2EMBED.DLL**
    - **Exploit: *integer overflow* dans le décompresseur LZCOMP**
      - **http://blogs.technet.com/srd/archive/2010/01/12/ms10-001-font-file-decompression-vulnerability.aspx**
    - **Crédit: Tavis Ormandy / Google**

Avis Microsoft (2/9)

- **MS10-002 Patch cumulatif pour IE (x8) [- / 1 / 1 / * / * / 1 / 2 / 1]**
  - *** Le patch MS09-072 protège contre l'exploitation de cette faille**
  - **Affecte: IE (toutes versions supportées)**
  - **Exploit: failles multiples, dont la fameuse faille "Aurora"**
    - **Contournement du filtre anti-XSS dans IE8**
    - ***Use-after-free* (x4)**
    - **Corruptions mémoire diverses (x3)**
    - **Voir également ZDI-10-011, ZDI-10-012, ZDI-10-013, ZDI-10-014**
  - **Crédit:**
    - **David Lindsay "thornmaker" & Eduardo A. Vela Nava "sirdarckcat"**
    - **Lostmon Lords**
    - **Brett Moore / ZDI**
    - **Wushi / team509**
    - **Sam Thomas / eshu.co.uk + ZDI (x2)**
    - **Haifei Li / Fortinet**
    - **Peter Vreugdenhil / ZDI**
    - **Meron Sellem / BugSec**

Avis Microsoft (3/9)

- **Remarque:**
  - **Patch hors cycle (21 janvier 2010)**
- **Lecture(s) complémentaire(s):**
  - **http://blogs.technet.com/srd/archive/2010/01/20/reports-of-dep-being-bypassed.aspx**
- **Sociétés ayant travaillé avec Microsoft suite à des attaques ciblées:**
  - **Google Inc.**
  - **MANDIANT**
  - **Adobe**
  - **McAfee**
  - **French government CSIRT (CERTA)**

Avis Microsoft (4/9)

- **Advisories**
  - **Q979267**
    - **Faille:**
      - **Vulnérabilités multiples dans la version de Flash 6 livrée avec Windows XP SP2/SP3**
    - **Correctif:**
      - **Désinstaller le lecteur ou installer la version la plus récente**
    - **Crédit:**
      - **TippingPoint / ZDI**
      - **Will Dormann / CERT/CC**
      - **Carsten H. Eiram & Dyon Balding / Secunia**

Avis Microsoft (5/9)

- Q979352
  - Faille dans Internet Explorer 6, 7 et 8
    - Accès incorrect à un objet libéré (*use after free*)
    - Exploitée en "0day" dans la nature (attaque "Aurora")
  - Crédit
    - Google, MANDIANT, Adobe et McAfee
  - Publiée dans la nature
    - http://wepawet.iseclab.org/view.php?hash=1aea206aa64ebeabb07237f1e2230d0f&type=js
  - Disponible dans Metasploit
    - http://blog.metasploit.com/2010/01/reproducing-aurora-ie-exploit.html

Avis Microsoft (6/9)

- La position officielle
  - http://blogs.technet.com/srd/archive/2010/01/15/assessing-risk-of-ie-0day-vulnerability.aspx
  - http://blogs.technet.com/msrc/archive/2010/01/17/further-insight-into-security-advisory-979352-and-the-threat-landscape.aspx
- Une bonne synthèse
  - http://extraexploit.blogspot.com/2010/01/iexplorer-0day-cve-2010-0249.html
- La communication autour de cette faille fait perdre des parts de marché à IE !
  - http://www.freenews.fr/spip.php?article7699

Avis Microsoft (7/9)

- Q979682
  - Elévation de privilèges locale par le biais du sous-système NTVDM
    - Ne fonctionne que sur les OS 32 bits
    - Reporté à Microsoft par Tavis Ormandy en juin 2009
    - Et finalement publié "dans la nature"
      - http://seclists.org/fulldisclosure/2010/Jan/341

- Q980088
  - Lecture de fichiers locaux arbitraires avec IE
  - (Hors mode protégé)
    - http://www.coresecurity.com/content/internet-explorer-dynamic-object-tag

Avis Microsoft (8/9)

- **Prévisions pour Février 2010**
  - **13 bulletins**
    - **26 vulnérabilités**
    - **5 bulletins critiques, 7 importants, 1 modéré**
    - **Windows (x11), Office < 2007 (x2)**
    - **http://blogs.technet.com/msrc/archive/2010/02/04/february-2010-bulletin-release-advance-notification.aspx**
  - **La faille NTVDM (Q979682) sera corrigée**
  - **La faille IE (Q980088) ne sera pas corrigée**
  - **Le déni de service sur SMB (Q977544) ne sera pas corrigé**

Avis Microsoft (9/9)

- Révisions
  - MS08-013
    - V1.4: correction de la liste des bulletins remplacés
  - MS09-035 (faille ATL)
    - V3.0: Windows Embedded CE 6.0 est affecté (!)
  - MS09-052
    - V1.2: correction d'une clé de BdR
  - MS09-060
    - V1.3: changement de la logique de détection
  - MS09-062
    - V2.2: mises à jour documentaires
  - MS09-073
    - V2.0: "Word" a été remplacé par "Office"
    - V2.1: corrections documentaires
  - MS10-002
    - V1.1: correction documentaire sur IE 5.01

Infos Microsoft

- **Sorties logicielles**
  - **Visual Studio 2010 / .NET 4.0 (en RC)**

Infos Microsoft

- **Autre**
  - **SDL: *Quick Security References***
    - **http://www.microsoft.com/downloads/details.aspx?FamilyID=79042476-951f-48d0-8ebb-89f26cf8979d**
      - **XSS**
      - **Injections SQL**
  - **SDL: implémentation simplifiée**
    - **http://www.microsoft.com/downloads/details.aspx?FamilyID=0baff8e8-ab17-4e82-a1ff-7bf8d709d9fb**
  - **Windows Seven 64 vs. BEEP.SYS**
    - **http://blogs.msdn.com/larryosterman/archive/2010/01/04/what-s-up-with-the-beep-driver-in-windows-7.aspx**
  - **De nouveaux records grâce à Seven**
    - **http://www.pcinpact.com/actu/news/55175-microsoft-benefice-record-windows-7.htm**
  - **Office 2010 ...**
    - **http://www.youtube.com/watch?v=UUYyocl_zgM**

Infos Réseau

- **Principales failles**
  - **PHP IDS**
    - **Exécution de code *PHP* arbitraire**
    - **Compte-tenu d'un appel non sûr à la fonction *unserialize()***
      - **http://www.sektioneins.com/en/advisories/advisory-022009-phpids-unserialize-vulnerability/**
  - **BIND < 9.6.1-P3 (et versions antérieures)**
    - **Empoisonnement de cache grâce à DNSSEC**
      - **https://www.isc.org/advisories/CVE2010-0097**
    - **Le patch original n'est pas suffisant**
      - **https://www.isc.org/node/504**
  - **MIT krb5**
    - ***Integer Overflow* dans l'implémentation AES et RC4**
      - **http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2009-004.txt**
  - **Solaris 10 Trusted Extension**
    - **... va charger une librairie utilisateur avec les droits *root***
      - **http://sunsolve.sun.com/search/document.do?assetkey=1-66-275410-1**

Infos Réseau

- Autres infos
  - 1.0.0.0/8 alloué
    - Mais il a fallu retirer 1.1.1.0/24 (et d'autres)
      - http://labs.ripe.net/content/pollution-18
  - La Chine se dispense de l'ICANN
    - Toutes les requêtes DNS sont désormais préfixées par ".cn"
      - http://www.internetactu.net/2010/01/26/le-grand-schisme-de-linternet/
    - Notez que l'Internet chinois est également passé à IPv6 ☺
  - mod_webfw2: un projet à surveiller ?
      - http://wiki.github.com/ellzey/mod_webfw2/wf2-configuration-syntax
  - Rapport Arbor Networks sur la sécurité réseau en 2009
    - Notez le DDoS de 49 Gbps
      - http://staging.arbornetworks.com/dmdocuments/ISR2009_EN.pdf

Infos Unix

- (Principales) failles
  - OpenSSL < 0.9.8m
    - Déni(s) de service
      - http://cvs.openssl.org/chngview?cn=19068
      - http://cvs.openssl.org/chngview?cn=19069
  - GnuTLS ne vérifiait pas les dates de révocation des certificats
      - http://www.bebt.de/debian/gnutls26/gnutls26_2.4.2-6+lenny3_i386.changes
  - Sun Ray 4.0 et 4.1
    - #1 exécution de code à distance avec les droits "root"
      - http://sunsolve.sun.com/search/document.do?assetkey=1-66-267548-1
    - #2 clés de chiffrement prédictibles
      - http://sunsolve.sun.com/search/document.do?assetkey=1-66-270549-1
    - Peut-on imaginer pire comme failles ... ?

Infos Unix

- Une faille dans le noyau Linux corrigée silencieusement
  - Affecte: Linux < 2.6.32.4
  - Exploit: DoS local au travers de do_mremap()
    - http://secunia.com/advisories/38229/
  - Même le CERTA s'est ému d'aussi peu de considération pour la sécurité !

- Samba #1
  - Affecte: Samba
  - Exploit: élévation de privilèges locale via mount.cifs
    - https://bugzilla.samba.org/show_bug.cgi?id=6853

- Samba #2
  - Si un dossier est accessible en écriture, l'attaquant peut créer un *symlink* et écrire sur tout le disque
    - http://seclists.org/fulldisclosure/2010/Feb/99
  - Ceci n'est pas une faille, mais une erreur de configuration (!)
    - "wide links = yes" par défaut sur toutes les distributions majeures

Infos Unix

- GZip
  - http://www.debian.org/security/2010/dsa-1974
- mod_proxy
  - Affecte: Apache 1.3 sur plateformes 64 bits
    - http://blog.pi3.com.pl/?p=69
- Le mois du 0day continue ...
  - Exécution de commandes arbitraires sur WebLogic via le port TCP/5556
    - http://intevydis.blogspot.com/2010/01/oracle-weblogic-1032-node-manager-fun.html
  - Le correctif
    - http://www.oracle.com/technology/deploy/security/alerts/alert-cve-2010-0073.html

Infos Unix

- **Autre**
  - **Fin de support pour Debian 4.0 au 15 février 2010**
  - **Apache 1.3 n'est plus supporté**
    - **(Sauf faille de sécurité énorme)**
    - **http://www.apache.org/dist/httpd/Announcement1.3.html**
  - **Le noyau 2.6.32 sera maintenu pendant 2+ ans**
    - **http://www.kroah.com/log/linux/stable-status-01-2010.html**
  - **GrSecurity sera maintenu aussi longtemps que le 2.6.32**
    - **http://article.gmane.org/gmane.linux.kernel.grsecurity/1084**
  - **Le site du CMS "e107" compromis et *backdooré***
    - **http://isc.sans.org/diary.html?storyid=8083**

Failles

- **Principales applications**
  - **La faille Acrobat Reader enfin corrigée**
    - **8 failles corrigées en tout**
      - **http://www.adobe.com/support/security/bulletins/apsb10-02.html**
      - **http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=836**
    - **Dont une disponible en "0day" dans Metasploit (!)**
      - **http://www.metasploit.com/redmine/projects/framework/repository/revisions/7617/entry/modules/exploits/windows/fileformat/adobe_u3d_meshdecl.rb**
    - **Et une autre triviale à exploiter (exécution de script dans un FDF)**
      - **http://archives.neohapsis.com/archives/fulldisclosure/2010-01/0245.html**
    - **Crédits:**
      - **Parvez Anwar / Secunia**
      - **Greg MacManus / iSIGHT Partners Labs**
      - **Code Audit Labs / iDefense**
      - **stratsec**
      - **Didier Stevens**
      - **Will Dormann / CERT**
      - **Nicolas Joly / VUPEN**

Failles

- Faille(s) dans QuickTime <= 7.6.4
  - Exploitée en "0day" dans la nature
    - http://www.offensive-security.com/blog/vulndev/multiple-media-player-http-datahandler-overflow/
    - http://www.securityfocus.com/bid/32540
    - http://www.exploit-db.com/exploits/11142
- Failles multiples dans Mac OS X
  - Avis 2010-001
    - http://support.apple.com/kb/HT4004
- Failles multiples dans iPhone OS < 3.1.3
    - http://support.apple.com/kb/HT4013
  - Dont la possibilité de changer les paramètres de configuration à distance
    - Si l'attaquant dispose de n'importe quel certificat SSL signé par une autorité connue
    - http://www.theregister.co.uk/2010/02/02/iphone_malicious_config_attack/

Failles

- **Failles multiples dans ThunderBird < 3.0.1**
  - **http://www.mozilla.org/security/announce/2009/mfsa2009-65.html**
  - **http://www.mozilla.org/security/announce/2009/mfsa2009-66.html**
  - **http://www.mozilla.org/security/announce/2009/mfsa2009-67.html**
- **Failles multiples dans ShockWave < 11.5.6.606**
  - **http://www.adobe.com/support/security/bulletins/apsb10-03.html**
- **Failles multiples dans RealPlayer**

Failles

- Oracle Quaterly Patch
  - 24 failles corrigées
    - http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2010.html
- WireShark < 1.2.6
- Aucune faille de sécurité corrigée dans Java 1.6.18
  - Juste 358 bogues ...
    - http://java.sun.com/javase/6/webnotes/6u18.html#bugfixes-1.6.0_18
- Un très mauvais générateur d'aléa embarqué dans des microcontrôleurs
  - Les impacts sont énormes (Zigbee, SmartGrid, etc.)
    - http://rdist.root.org/2010/01/11/smart-meter-crypto-flaw-worse-than-thought/

Failles 2.0

- Baidu.cn "piraté"
  - Même technique (vol de l'entrée DNS) et mêmes auteurs que pour Twitter
    - http://garwarner.blogspot.com/2010/01/iranian-cyber-army-returns-target.html
  - Remarque: Baidu == plus gros moteur de recherche chinois
    - Plus de 70% du marché
- Du côté des XSS
  - TagCloud.swf (34 millions de pages concernées)
    - http://websecurity.com.ua/3842/
  - Twitter et Google Calendar
    - Pas trivial à exploiter dans des conditions "réelles"
    - http://www.infosecurity-magazine.com/view/6202/twitter-and-google-calendar-xss-vulnerabilities-revealed/

Failles 2.0

- Un "antivirus" sous forme d'application Facebook
  - http://community.websense.com/blogs/websense-features/archive/2010/01/20/websense-introduces-first-real-time-security-application-for-facebook.aspx?cmpid=prnr
- Obscurcissement (trivial) de lien sous Safari et Chrome
  - http://nomoreroot.blogspot.com/2010/01/little-bug-in-safari-and-google-chrome.html
- Mots de passe 2.0: rien n'a changé
  - Une analyse des 32 millions de mots de passe "RockYou"
  - Résultat: "123456" est toujours premier
    - http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf

Malwares et spam

- Des plugins FireFox infectés
  - Et distribués pendant plusieurs mois ...
    - http://blog.mozilla.com/addons/2010/02/04/please-read-security-issue-on-amo/
- Etude des applications malveillantes sur BlackBerry
  - Attention: rien d'exceptionnel dans ce papier
    - http://threatcenter.smobilesystems.com/?p=1752
- Rapport de l'ENISA
  - Etude comparative des méthodes anti-spam chez les FAI européens
    - http://www.enisa.europa.eu/act/res/other-areas/anti-spam-measures/studies/spam-survey/at_download/fullReport

Actualité (France)

- ANSSI – Conseils aux voyageurs
  - http://www.securite-informatique.gouv.fr/gp_article712.html
  - http://www.securite-informatique.gouv.fr/IMG/pdf/Passeport-de-conseils-aux-voyageurs_janvier-2010.pdf
- Le décret d'application du RGS publié au JO
  - http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021779444
- IDéNUM: une identité numérique encadrée par le gouvernement ?
  - http://www.telecom.gouv.fr/actualites/1-fevrier-2010-label-idenum-identite-numerique-multi-services-2311.html
  - Quelques problèmes à l'allumage néanmoins
    - http://www.pcinpact.com/actu/news/55219-idenum-identite-numerique-internet-domaine.htm
- 9 et 10 février: vote de la LOPPSI 2
  - A lire avant de voter
    - http://fr.readwriteweb.com/2010/01/29/a-la-une/loppsi-pedophiles-business-analyse/

Actualité (France)

- 35% des dirigeants français vont maintenir ou augmenter le budget sécurité en 2010
  - http://www.decision-achats.fr/Breves/Securite-informatique-seuls-35-des-decideurs-fran-ais-vont-maintenir-ou-augmenter-leur-budget-en-2010-31756.htm
- CLUSIF – Panorama de la cybercriminalité - Bilan de l'année 2009
  - http://www.clusif.asso.fr/fr/production/ouvrages/pdf/PanoCrim2k9-fr.pdf
- Phishing (amateur) sur la Caisse d'Epargne
  - http://www.zataz.com/alerte-phishing/19801/caisse-epargne-phishing-hameconnage.html
- Le certificat SSL de LaPoste.net expire

Actualité (anglo-saxonne)

- Un "cyber exercice" du 9 au 11 février
  - Ciblant les institutions de paiement
    - http://www.securityfocus.com/brief/1059
- "US Cybersecurity Enhancement Act"
    - http://www.v3.co.uk/v3/news/2257369/cybersecurity-enhancement-act
- Citigroup piraté depuis plus d'un an (?)
    - http://www.itespresso.fr/securite-it-la-banque-americaine-citigroup-victime-dune-cyber-attaque-32951.html
- "Il faut utiliser un PC dédié aux opérations bancaires"
  - Source: *American Bankers' Association*
    - http://blog.tenablesecurity.com/2010/01/afterbytes-with-marcus-ranum-using-a-dedicated-pc-for-online-banking.html
- Gartner rachète Burton Group
    - http://www.zdnet.fr/actualites/informatique/0,39040745,39711981,00.htm

Actualité (européenne)

- **Projet d'accord entre l'Europe et les USA sur la protection des données personnelles**
  - **http://ec.europa.eu/justice_home/news/consulting_public/wai/news_consulting_0005_en.htm**

- **Un cyber-exercice européen en novembre 2010 (?)**
  - **http://www.enisa.europa.eu/media/news-items/1st-pan-european-ciip-excercises**

Actualité (Google)

- Failles multiples dans Chrome < 4.0.249.78 (x11)
  - http://googlechromereleases.blogspot.com/2010/01/stable-channel-update_25.html
  - Voir aussi: Alex Sotirov
    - http://www.phreedom.org/chrome.png
- Google offre $1337 par bogue dans Chrome
  - http://blog.chromium.org/2010/01/encouraging-more-chromium-security.html
- Google Apps ne supportera bientôt plus IE6
  - http://googleenterprise.blogspot.com/2010/01/modern-browsers-for-modern-applications.html
- Google fait appel à la NSA pour se protéger ...
  - http://www.wired.com/threatlevel/2010/02/google-seeks-nsa-help/

Actualité (Google)

- La Google Toolbar est un spyware
  - Mais il s'agit d'un bogue logiciel qui a été rapidement corrigé
    - http://www.zdnet.fr/actualites/internet/0,39020774,39712553,00.htm
- Google remplacé par Bing dans la configuration par défaut des iPhones ?
    - http://www.cnetfrance.fr/news/apple-microsoft-bing-39712355.htm
- Google Energy va devenir producteur et fournisseur d'électricité
    - http://www.greenit.fr/article/energie/google-va-devenir-un-fournisseur-d-energie

Actualité (crypto)

- Les CB attaquées par un chercheur anglais
  - Dans certaines conditions, il est possible de simuler la saisie du code PIN auprès du terminal de paiement
    - http://www.liberation.fr/economie/0101614961-cartes-a-puce-les-banques-mobilisees-contre-un-risque-de-fraude
- JSCrypto double FAIL == WIN
    - http://corte.si/posts/security/jscrypto.html
- La cryptographie quantique n'est pas inviolable
  - Attaque "man in the middle"
    - http://pro.01net.com/editorial/510714/une-faille-dans-les-systemes-de-chiffrement-quantique/

Actualité (crypto)

- RFID FAIL ... *again*
  - Le système "Legic Prime" a été démonté
  - Il est utilisé entre autres ... pour contrôler l'accès aux centrales nucléaires
    - http://blogs.ict-forward.eu/forward/security-system-%E2%80%9Clegic-prime%E2%80%9D-hacked/
- L'algorithme Kasumi (A5/3 – réseaux 3G) menaçé
  - http://threatpost.com/en_us/blogs/second-gsm-cipher-falls-011110

Actualité

- "Opération Aurora"
  - Difficile de démêler le vrai du faux ...
    - http://www.wired.com/threatlevel/2010/01/hack-of-adob/
    - http://siblog.mcafee.com/cto/operation-%E2%80%9Caurora%E2%80%9D-hit-google-others/
  - Ce qui est sûr
    - Il existait une faille non patchée dans Internet Explorer
      - Q979352
    - Cette faille a été largement exploitée dans la nature
      - 30+ sociétés américaines visées
    - Les attaquants s'intéressaient principalement aux codes sources
      - http://www.wired.com/threatlevel/2010/01/google-hack-attack/
    - Les données ont transité par RackSpace avant de partir pour Taiwan
      - http://www.rackspace.com/blog/?p=800

Actualité

- La position d'Adobe
  - http://blogs.adobe.com/asset/2010/01/further_details_regarding_atta.html
  - http://blogs.adobe.com/conversations/2010/01/adobe_investigates_corporate_n.html
- La position de Google
  - http://googleblog.blogspot.com/2010/01/new-approach-to-china.html
  - http://googleenterprise.blogspot.com/2010/01/keeping-your-data-safe.html
- La position de Schneier
  - C'est le système d'interception légale de GMail qui a été piraté !
    - http://edition.cnn.com/2010/OPINION/01/23/schneier.google.hacking/index.html
- La preuve de l'implication de la Chine ?
  - http://www.secureworks.com/research/blog/index.php/2010/1/20/operation-aurora-clues-in-the-code/

Actualité

- L'ajout d'une autorité de certification chinoise dans Firefox fait débat
  - https://bugzilla.mozilla.org/show_bug.cgi?id=476766
  - http://lwn.net/Articles/372264/
- Un site (payant) d'entrainement au hacking fermé par la police chinoise
  - 170 000 utilisateurs
  - 12 000 utilisateurs payants
    - http://news.yahoo.com/s/ap/20100208/ap_on_bi_ge/as_china_hacking
- Une affaire de vol d'informations sur des réserves pétrolières fait surface
  - Les faits ont plus de 3 ans
    - http://www.wired.com/threatlevel/2010/01/hack-for-oil
- La bourse carbone européenne attaquée par des pirates
  - Vol de mots de passe par *phishing*
    - http://www.jdf.com/matieres-premieres/2010/02/02/02004-20100202ARTJDF00006-cyberattaque-sur-le-marche-du-co.php

Actualité

- Guide de sécurisation pour VMWare vSphere (ESX 4)
  - http://blogs.vmware.com/security/2010/01/announcing-vsphere-40-hardening-guide-public-draft-release.html
- Campus Party Europe / Network Security
  - Du 14 au 18 avril à Madrid
    - http://www.campus-party.eu/NetworkSecurity.html
- FAA: "le prochain Boeing devra résister aux hackers"
  - Mais comment ... ?
    - http://blog.seattlepi.com/aerospace/archives/191558.asp
- Sorties logicielles
  - Nmap 5.20 (puis 5.21)
  - FireFox 3.6

Fun

- La PS3 compromise
  - Après 3 ans de recherches ...
    - http://geohotps3.blogspot.com/2010/01/heres-your-silver-platter.html
  - Explication
    - http://rdist.root.org/2010/01/27/how-the-ps3-hypervisor-was-hacked/
  - Explication pour les masses
    - http://www.eurogamer.net/articles/digitalfoundry-ps3hacked-article
- Avec la crise, les informaticiens doivent remettre la cravate
    - http://www.lefigaro.fr/lentreprise/2009/04/16/09001-20090416ARTFIG00609-comprenez-vous-le-dress-code-de-votre-entreprise-.php
- Le piratage d'un panneau publicitaire interactif provoque un embouteillage géant
  - Un clip porno était diffusé
    - http://en.rian.ru/russia/20100115/157558900.html
- *3001#12345#* marche aussi sur iPhone
    - http://www.tuaw.com/2007/07/12/more-secret-iphone-codes/

Questions / réponses

- Questions / réponses
- Conférence JSSI
  - Mardi 16 mars 2010
- Prochaine réunion
  - Mardi 13 avril 2010
- N'hésitez pas à proposer des sujets et des salles