OSSIR
Groupe Paris

Réunion du 13 octobre 2009

Revue des dernières vulnérabilités

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

Avis Microsoft (1/7)

- **Correctif de Septembre 2009**
  - **Avec [exploitability index]**
  - **A lire également:**
    - **http://blogs.technet.com/srd/archive/2009/09/08/assessing-the-risk-of-the-september-critical-security-bulletins.aspx**
    - **http://blogs.technet.com/msrc/archive/2009/09/08/september-2009-security-bulletin-release.aspx**
    - **http://blogs.technet.com/msrc/archive/2009/09/11/september-2009-security-bulletin-webcast-video-and-customer-q-and-a.aspx**
    - **http://blogs.technet.com/msrc/pages/monthly-security-bulletin-webcast-q-a-september-2009.aspx**
  - **MS09-045 Faille dans le moteur JScript [1]**
    - **Affecte: JScript 5.1 – 5.8**
      - **Donc Windows (toutes versions supportées, sauf Seven et 2008 R2)**
    - **Exploit: exécution de code (natif) via un script malformé**
      - **Exploitable via une page Web**
    - **Crédit: Wushi / team509 via ZDI**

Avis Microsoft (2/7)

- **MS09-046 Faille dans le composant ActiveX "DHTML Editor" [2]**
  - **Affecte: Windows 2000 / XP / 2003**
  - **Exploit:**
  - **Crédit: Tavis Ormandy / Google**

- **MS09-047 Failles dans les codecs Windows Media (x2) [1,1]**
  - **Affecte: Windows Media Runtime 9.0 – 11.0**
    - **Donc Windows (toutes versions supportées, sauf Seven et 2008 R2)**
  - **Exploit:**
    - **Fichier ASF malformé**
    - **FIchier MP3 malformé**
  - **Crédit:**
    - **Peter Winter-Smith / NGS Software**
    - **Hiroshi Noguchi / Alice Carroll fan club**

Avis Microsoft (3/7)

- MS09-048 Failles dans la pile TCP/IP (x3) [3,2,3]
  - Affecte: Windows (toutes versions supportées, sauf Seven et 2008 R2)
  - Exploit:
    - Déni de service par taille de fenêtre nulle
      - CVE-2008-4609, voir plus loin
    - Exécution de code à distance via les timestamps TCP
    - Déni de service via des connexions TCP orphelines
      - http://www.recurity-labs.com/content/pub/Microsoft_Windows_CVE-2009-1926_MS09-048.txt
  - Crédit:
    - Jack C. Louis / Outpost24
    - Fabian Yamaguchi / Recurity Labs
  - Notes:
    - Aucun correctif disponible pour Windows 2000 et Windows XP (!)
    - http://blogs.technet.com/srd/archive/2009/09/08/ms09-048-tcp-ip-vulnerabilities.aspx
  - De nouvelles protections ajoutées contre la surconsommation de ressources
    - http://support.microsoft.com/kb/974288

Avis Microsoft (4/7)

- **MS09-049 Faille dans le service "Wireless LAN Autoconfig" (wlansvc) [2]**
  - **Affecte: Windows Vista / 2008**
  - **Exploit: exécution de code à la réception d'une trame WiFi malformée**
  - **Crédit: n/d**

Avis Microsoft (5/7)

- **A noter également**
  - **Changement (optionnel) du fonctionnement AutoPlay dans Windows XP**
    - **http://blogs.technet.com/srd/archive/2009/09/11/autoplay-windows-7-behavior-backported.aspx**
    - **http://support.microsoft.com/kb/971029**
  - **Mise à jour GDI+ permettant de choisir les formats supportés**
    - **http://support.microsoft.com/kb/958911**
- **Prévisions pour Octobre 2009**
  - **13 bulletins en vue ...**

Avis Microsoft (6/7)

- Advisories
  - 975497: faille SMBv2
    - V1.1: mise à jour de la FAQ
    - V1.2: mise à jour de la FAQ

Avis Microsoft (7/7)

- **Révisions**
  - **MS09-038**
    - **V1.1: correction du *workaround***
  - **MS09-045**
    - **V1.1: correction du nom de fichier sur Windows 2003 x64**
    - **V1.2: précisions sur la désinstallation du correctif**
  - **MS09-047**
    - **V1.1: correction de la liste des bulletins remplacés**
  - **MS09-048**
    - **V2.0: Windows XP est affecté, mais ne sera pas corrigé**
    - **V2.1: mise à jour de la FAQ**
  - **MS09-049**
    - **V1.1: précisions sur les conditions d'exploitation**

Infos Microsoft

- **Sorties logicielles**
  - **De nouveaux outils pour appliquer le SDL**
    - **BinScope Analyzer**
      - **http://www.microsoft.com/downloads/details.aspx?FamilyID=90E6181C-5905-4799-826A-772EAFD4440A**
    - **MiniFuzzer**
      - **http://www.microsoft.com/downloads/details.aspx?FamilyID=b2307ca4-638f-4641-9946-dc0a5abe8513**
  - **Librairie anti-XSS version 3.1**
    - **http://blogs.msdn.com/sdl/archive/2009/09/23/new-and-improved-antixss-3-1-now-with-sanitization.aspx**
  - **Exchange 2007 SP2**
  - **"Windows XP Mode" pour Windows Seven en RTM**

Infos Microsoft

- **Autre**
  - **Windows Server 2008 Hyper-V certifié EAL4+**
    - **Par le BSI allemand**
  - **Quelques statistiques sur les programmes Microsoft**
    - **Moins de 13% des failles trouvées par le programme MSVR dans des produits tiers ont été corrigées !**
      - **http://download.microsoft.com/download/4/2/7/427A9ED7-B521-4A70-B40A-AC4937BC5092/Information_Sharing_and_MSRC.pdf**
  - **Mieux vaut réinstaller son système !**
    - **http://blog.tune-up.com/windows-os/windows-7-performance-check-upgrade-install-vs-clean-install/**
  - **Ouverture du Windows Café à Paris le 22 octobre**
    - **http://www.pcinpact.com/actu/news/53165-windows-cafe-paris-microsoft.htm**

Infos Microsoft

- Windows 8 sera un système 128 bits
  - (Grâce à une fuite sur LinkedIn)
    - http://www.pcpro.co.uk/news/enterprise/352270/microsoft-leaks-details-of-windows-8-and-windows-9
- PowerShell en tant que *shell* Emacs
    - http://blogs.msdn.com/dotnetinterop/archive/2008/04/10/powershell-in-emacs-proof.aspx
- Les utilisateurs du téléphone SideKick de Microsoft perdent toutes leurs données
    - http://www.pcinpact.com/actu/news/53546-sidekick-tmobile-microsoft-danger-pertes.htm
- Le choc interculturel
  - "Windows Seven launch parties"
    - http://www.youtube.com/watch?v=9oWWt_L-qeo

Infos Réseau

- **Principales failles**
  - **"La" faille TCP corrigée (CVE-2008-4609)**
    - **https://www.cert.fi/haavoittuvuudet/2008/tcpvulnerabilitiesstatement.html**
    - **https://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html**
  - **Produits corrigés**
    - **Windows Vista (et ultérieur)**
      - **MS09-048**
    - **Cisco**
      - **http://www.cisco.com/warp/public/707/cisco-sa-20090908-tcp24.shtml**
    - **CheckPoint**
      - **https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=42723**
      - **https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=42725**
    - **Solaris (plus tard)**
      - **http://sunsolve.sun.com/search/document.do?assetkey=1-66-267088-1**

Infos Réseau

- Produits non corrigés
  - Windows 2000 et XP
  - RedHat
    - http://kbase.redhat.com/faq/docs/DOC-18730

Autres failles

- Sortie des correctifs semestriels chez Cisco
  - http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep09.html
- Déni de service dans FreeRADIUS < 1.1.8
  - https://lists.freeradius.org/pipermail/freeradius-users/2009-September/msg00242.html
- Dnsmasq < 2.50

Infos Réseau

- **Autres infos**
  - **Snort Emerging Threats**
    - **Une modification de la configuration Snort à prévoir**
      - **http://www.emergingthreats.net/index.php/component/content/article/17-sigs/203-rule-file-change-coming.html**
  - **IETF: "Recommendations for the Remediation of Bots in ISP Networks"**
    - **http://tools.ietf.org/html/draft-oreirdan-mody-bot-remediation-03**
  - **La version finale de 802.11n approuvée**
    - **http://www.networkworld.com/news/2009/091109-80211n-approved.html**
  - **+1400% pour IPv6 en 1 an**
    - **Depuis Teredo et ... uTorrent !**
      - **http://asert.arbornetworks.com/2009/09/who-put-the-ipv6-in-my-internet/**

Infos Réseau

- COLT: la panne géante
  - http://twitter.com/COLToutagenews
- Comcast doit-il alerter ses utilisateurs en cas d'activité suspecte ?
  - Une fausse bonne idée ?
    - http://tech.yahoo.com/news/ap/20091009/ap_on_hi_te/us_tec_comcast_virus_2

Infos Unix

- (Principales) failles
  - Déni de service distant dans le noyau Linux
    - Via un paquet AppleTalk
      - http://git.kernel.org/?p=linux/kernel/git/davem/net-next-2.6.git;a=commit;h=ffcfb8db540ff879c2a85bf7e404954281443414
  - Faille dans Linux 2.6.31
    - perf_copy_attr()
    - Et gros troll en perspective ...
      - http://lwn.net/Articles/353976/
  - Faille dans KVM
    - Exploitable ou pas ?
      - http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=07708c4af1346ab1521b26a202f438366b7bcffd
      - http://twitter.com/spendergrsec/statuses/4076850005

Infos Unix

- Faille(s) dans Horde < 3.3.5, < 3.2.5
  - http://www.sektioneins.de/advisories/SE-2009-01.txt
  - http://marc.info/?l=horde-announce&m=125291625030436&w=2
  - http://marc.info/?l=horde-announce&m=125292339907481&w=2
- Faille(s) dans Samba 3.x
  - http://www.samba.org/samba/security/CVE-2009-2948.html
  - http://www.samba.org/samba/security/CVE-2009-2906.html
  - http://www.samba.org/samba/security/CVE-2009-2813.html
- "gcc -mudflap" : pas si sûr que ça ...
  - http://c-skills.blogspot.com/2009/09/gcc-fmudflap.html
- "Faille" dans Xen
  - pyGrub ne vérifie pas le mot de passe de boot ...
    - http://rhn.redhat.com/errata/RHSA-2009-1472.html

Infos Unix

- **Nouvelle faille kqueue() dans FreeBSD**
  - **http://seclists.org/fulldisclosure/2009/Sep/0141.html**
- **Autres failles FreeBSD en vrac ...**
  - **Faille #1**
    - **http://security.freebsd.org/advisories/FreeBSD-SA-09:13.pipe.asc**
    - **http://www.frasunek.com/pipe.txt**
  - **Faille #2**
    - **http://security.freebsd.org/advisories/FreeBSD-SA-09:14.devfs.asc**
    - **http://www.frasunek.com/devfs.txt**
- ***Heap overflow* dans la commande "w" (!)**
  - **Affecte: Solaris (toutes versions)**
    - **http://sunsolve.sun.com/search/document.do?assetkey=1-66-266348-1**

Infos Unix

- **Autre**
  - La *roadmap* de GrSecurity
    - http://permalink.gmane.org/gmane.linux.kernel.grsecurity/1060
  - SELinux + clustering = FAIL sur RedHat
    - http://marc.info/?l=selinux&m=125244025732144&w=2
    - https://bugzilla.redhat.com/show_bug.cgi?id=503141
  - Le noyau Linux devient "*bloated & huge*"
    - http://www.theregister.co.uk/2009/09/22/linus_torvalds_linux_bloated_huge/
  - GDB 7 supportera le "*reverse debugging*"
    - http://www.gnu.org/software/gdb/news/reversible.html
  - Un portage d'APT en ... PERL
    - http://wiki.debian.org/Cupt

Failles

- **Principales applications**
  - **FireFox < 3.0.14, < 3.5.3**
    - **Note: la dernière version de FireFox contrôle automatiquement la version du plugin Flash**
  - **Google Chrome < 3.0.195.21 ^H^H^H .24**
    - **http://googlechromereleases.blogspot.com/2009/09/stable-channel-update.html**
    - **http://googlechromereleases.blogspot.com/2009/09/stable-channel-update_30.html**
  - **Faille(s) dans Acrobat Reader (toutes versions)**
    - **Exploitées en "0day" sur Internet**
    - **http://blogs.adobe.com/psirt/2009/10/adobe_reader_and_acrobat_issue_1.html**
    - **http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=826**
    - **http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=827**
  - **WireShark < 1.2.2, < 1.0.9**
    - **http://www.wireshark.org/security/wnpa-sec-2009-06.html**
  - **VLC < 1.0.2**
    - **http://www.videolan.org/security/sa0901.html**

Failles

- Encore un paquet de failles corrigées dans ...
  - Mac OS X
    - http://support.apple.com/kb/HT3865
    - http://support.apple.com/kb/HT3864 (mise à jour Flash pour 10.6)
  - iPhone / iPod
    - http://support.apple.com/kb/HT3860
  - QuickTime (< 7.6.4)
    - http://support.apple.com/kb/HT3859
  - iTunes < 9.0.1
    - http://support.apple.com/kb/HT3884
- Mac OS 10.6 supporte mal le compte "guest"
    - http://reviews.cnet.com/8301-13727_7-10346974-263.html
- Quelques failles venues du froid
  - Adobe RoboHelp Server 8
    - http://www.intevydis.com/blog/?p=69
  - Kaspersky Online Antivirus
    - http://www.intevydis.com/blog/?p=77

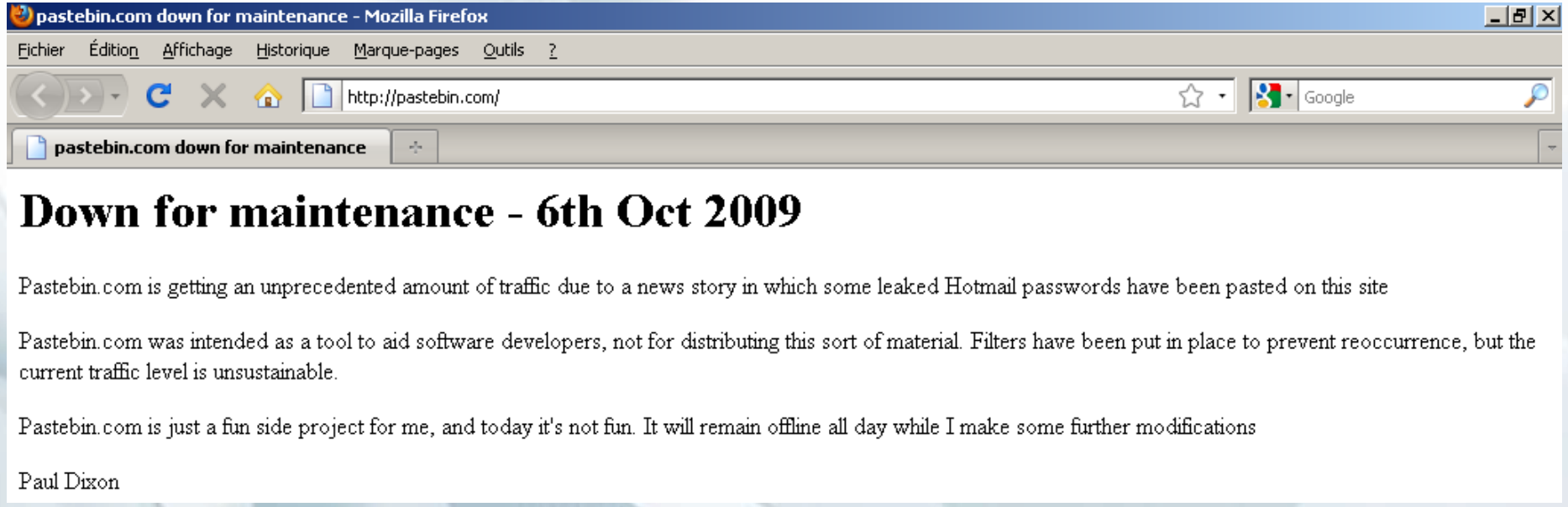
Failles

- Elévation de privilèges possible si VMWare Fusion est installé
  - Affecte: VMWare Fusion < 2.0.5
    - http://lists.vmware.com/pipermail/security-announce/2009/000066.html
- Le BlackBerry également vulnérable aux certificats SSL contenant un caractère NULL
    - http://www.blackberry.com/btsc/viewContent.do?externalId=KB19552&sliceId=1
- "Une vulnérabilité a été découverte dans IBM Informix Dynamic Server. Un utilisateur se connectant avec un mot de passe de 512 caractères ou plus peut provoquer un déni de service."
    - http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-411/CERTA-2009-AVI-411.html
- Un certificat SSL délivré pour '*' disponible
    - https://www.noisebridge.net/pipermail/noisebridge-discuss/2009-September/008400.html

Failles 2.0

- 10,000 mots de passe Hotmail retrouvés "par hasard" sur pastebin.com
  - Question : s'en serait-on rendu compte autrement ?
    - http://www.theregister.co.uk/2009/10/05/hotmail_passwords_leaked/

- Effet de bord ...



Failles 2.0

- Le WAF dans l'application
  - Avec la nouvelle version de OWASP ESAPI
    - http://www.darkreading.com/security/app-security/showArticle.jhtml?articleID=220100630

- Mots de passe et Web 2.0, c'est toujours l'échec ...
  - http://no.spam.ee/~tonu/passwords.html

```
mysql> select password, sex, c
+------------+------+-------+
| password   | sex  | c     |
+------------+------+-------+
| 123456     | M    | 17601 |
| password   | M    |  4545 |
| 12345      | M    |  3480 |
| 1234       | M    |  2911 |
| 123        | M    |  2492 |
| 123456789  | M    |  2225 |
| 123456     | F    |  1885 |
| qwerty     | M    |  1883 |
| 12345678   | M    |  1791 |
```

Failles 2.0

- Month of Facebook Bugs
  - http://theharmonyguy.com/
- Erreur grossière dans l'API Yahoo
  - Le Web Services permet l'énumération de comptes
    - http://tacticalwebappsec.blogspot.com/2009/09/distributed-brute-force-attacks-against.html
- Falsification des signatures dans l'API Flickr
  - http://netifera.com/research/flickr_api_signature_forgery.pdf
- Méfiez-vous du "/.svn"
  - http://translate.google.com/translate?hl=ru&sl=ru&tl=en&u=http%3A%2F%2Fhabrahabr.ru%2Fblogs%2Finfosecurity%2F70330%2F

Failles 2.0

- ASmallWorld.com piraté
  - Par des français qui exigeaient une rançon de $1m
    - http://www.avertlabs.com/research/blog/index.php/2009/09/17/private-jet-set-network-hacked/
- Un cambrioleur arrêté grâce à Facebook
    - http://www.infos-du-net.com/actualite/16003-Facebook-fait-divers.html

Malwares et spam

- W32/Xpaj: un infecteur d'exécutables innovant
  - http://www.avertlabs.com/research/blog/index.php/2009/09/21/w32xpaj-know-your-polymorphic-enemy/
- Après Twitter, au tour de Google Groups
  - De servir de canal C&C pour un malware !
    - http://www.symantec.com/connect/blogs/google-groups-trojan
- Le modèle Open Source creuse son trou chez les auteurs de malwares
  - http://software.silicon.com/security/0,39024655,39525925,00.htm
- Les machines infectées le restent longtemps
  - 50% des machines infectées le sont depuis plus d'un an
    - http://www.h-online.com/security/Internet-security-many-PC-infections-are-long-term--/news/114273

Malwares et spam

- Un test indépendant (donc intéressant) sur l'efficacité des antivirus
  - http://www.nsslabs.com/anti-malware
  - http://blog.metasploit.com/2009/09/nss-labs-endpoint-protection-test.html
- Communication des éditeurs
  - Symantec
    - http://www.youtube.com/watch?gl=US&v=0o8XMlL8rqY

Actualité (France)

- HADOPI finalement votée
  - Déjà des dommages collatéraux ?
    - http://www.itespresso.fr/piratage-du-site-odebi-degat-collateral-de-la-loi-hadopi-31359.html
- Edu4 vs. AFPA
  - Un jugement historique pour la GPL en France
    - http://fsffrance.org/news/article2009-09-22.fr.html
- Neutralité du Net: le débat est loin d'être clos
    - http://www.laquadrature.net/fr/neutralite-du-net-lettre-aux-ministres-concernes
- Arkoon rachète SkyRecon
    - http://www.securityvibes.com/arkoon-skyrecon-jsaiz-news-3003379.html

Actualité (France)

- Linux 2.6.27 / netfilter / iptables 1.4.2 certifié au titre de la CSPN
  - http://www.ssi.gouv.fr/site_rubrique54_certificat_cspn_2009_04.html
- Un hyperviseur certifié EAL5
  - http://securite.reseaux-telecoms.net/actualites/lire-la-dga-durcit-la-securite-de-son-hyperviseur-de-virtualisation-20905.html
- L'INRIA ouvre un centre de recherche consacré aux logiciels libres
  - http://www.zdnet.fr/actualites/informatique/0,39040745,39708326,00.htm
- Zataz condamné en appel
  - http://www.zataz.com/news/19509/zataz--jugement-sur-la-forme.html
- Les français s'illustrent encore
  - http://www.t2.fi/2009/10/05/t209-challenge-winners/

Actualité (France)

- Plusieurs campagnes de *phishing* actives en France
  - Impôts, CAF, ...
- Vite! La grippe!
  - http://www.myglobull.fr/h1n1-entreprises.html
- La langue française s'enrichit
  - http://www.20minutes.fr/article/345703/France-Arrosage-filoutage-et-fouineur-les-nouveaux-mots-de-l-Internet-en-francais.php
- Les programmes "innovants" du Web 2.0 français
  - http://www.telecom.gouv.fr/rubriques-menu/soutiens-financements/programmes-nationaux/volet-numerique-du-plan-relance/resultats-deux-appels-projets/liste-projets-retenus-web-innovant-2218.html

Actualité (anglo-saxonne)

- Le SANS publie les "top security risks" du mois de septembre
  - http://www.sans.org/top-cyber-security-risks/
- Le SANS donne également accès aux statistiques de ses "Web honeypots"
  - http://isc.sans.org/weblogs/
- Le "Virtual Private Cloud"
  - http://aws.amazon.com/vpc/

Actualité (Google)

- Google achète la société reCAPTCHA
  - Désormais les CAPTCHA aideront à numériser des livres !
    - http://news.slashdot.org/story/09/09/17/1238226/Google-Buys-reCAPTCHA-For-Better-Book-Scanning
- Quand GMail mélange les emails
    - http://news.cnet.com/8301-27080_3-10356803-245.html
- Google Chrome Frame: le débat s'enflamme
    - http://code.google.com/chrome/chromeframe/
- Google Chrome OS
    - http://sites.google.com/site/chromeoslinux/

Actualité (Google)

- Android vulnérable aux SMS malformés
  - Un simple déni de service grâce à l'utilisation de Java
    - http://article.gmane.org/gmane.comp.security.oss.general/2160
- Comment s'affranchir de Google ?
  - C'est possible !
    - http://www.dataliberation.org/home
- Des emails issus d'un compte supprimé produits par Google lors d'un procès
    - http://dealbook.blogs.nytimes.com/2009/10/09/email-shows-fear-of-blow-up-risk-at-bear-fund/

Actualité

- **Mozilla Plugin Check**
  - **Une vraie bonne idée**
    - **https://www-trunk.stage.mozilla.com/en-US/plugincheck/**
- **La fin des certificats gratuits chez Thawte**
    - **https://search.thawte.com/support/ssl-digital-certificates/index?page=content&id=AD196&actp=LIST&viewlocale=en_US**
- **XySSL devient PolarSSL**
    - **http://polarssl.org/**

Fun

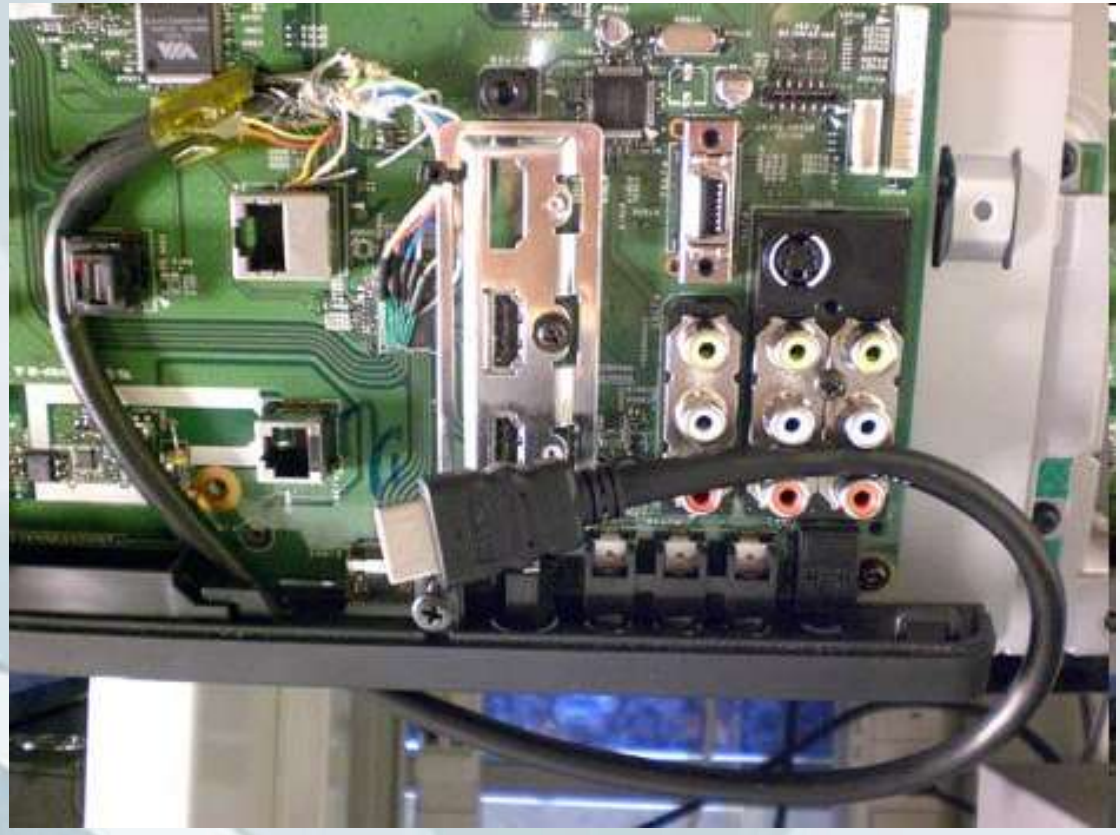
- HaikuOS passe en Alpha1
  - Après 8 ans de développement
    - http://www.haiku-os.org/news/2009-09-13_haiku_project_announces_availability_haiku_r1alpha_1
- Ce que Star Trek apporte à la sécurité informatique
    - http://ha.ckers.org/blog/20090918/what-star-trek-predicts-about-the-future-of-information-security/
- La performance des réseaux africains en question
    - http://idle.slashdot.org/story/09/09/10/0318203/Pigeon-Turns-Out-to-be-Faster-Than-S-African-Net
- Le comble de la mauvaise foi
  - Sur les questions d'Open Source
    - http://news.zdnet.co.uk/itmanagement/0%2C1000000308%2C39760362%2C00.htm

Fun

- Le piratage des robots domestiques, une future menace
  - https://www.cs.washington.edu/research/security/robots/
- Un pirate informatique nommé administrateur réseau dans sa prison
  - Du coup il pirate le système interne ☺
    - http://www.mirror.co.uk/news/top-stories/2009/09/27/conputer-meltdown-115875-21703149/
- Ruby sait diviser par zéro
  - http://banisterfiend.wordpress.com/2009/10/02/wtf-infinite-ranges-in-ruby/
- Une peinture pour bloquer les ondes radio
  - http://www.numerama.com/magazine/14117-ondes-radios-une-peinture-speciale-anti-wi-fi.html

Fun

- HDCP contourné
  - Avec quelques fils
    - http://hackaday.com/2009/10/01/tv-hack-bypasses-hdcp/



Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 10 novembre 2009
- N'hésitez pas à proposer des sujets et des salles