OSSIR
Groupe Paris

Réunion du 9 septembre 2008

Revue des dernières vulnérabilités

EdelWeb

Olivier REVENU
olivier.revenu (à) edelweb.fr

Mickaël DEWAELE
mickael.dewaele (à) edelweb.fr

Jérémy LEBOURDAIS
jeremy.lebourdais (à) edelweb.fr

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

Avis Microsoft (1/15)

- **Correctifs de Juillet 2008**
  - **MS08-037 Faille(s) DNS**
    - **Affecte : Windows toutes versions supportées**
      - **D'autres constructeurs sont impactés : Cisco, BIND ...**
    - **Exploit(s) :**
      - **CVE-2008-1447**
      - **CVE-2008-1454**
      - **Des informations intéressantes sur la clé MaxUserPort**
        - **http://blogs.technet.com/swi/archive/2008/07/08/ms08-037-more-entropy-in-the-dns-resolver.aspx**
    - **Crédit : Dan Kaminsky / IOActive**
    - **Remarque :**
      - **"La" faille du buzz ...**

Avis Microsoft (2/15)

- MS08-038 Faille dans Windows Explorer
  - Affecte : Windows Vista et 2008
  - Exploit :
    - Fichier de recherche sauvegardée malformé (".search-ms")
    - Corrige également le support de la clé "NoDriveTypeAutorun"
      - http://www.kb.cert.org/vuls/id/889747
  - Crédit : n/d

- MS08-039 Cross-site scripting dans OWA (x2)
  - Affecte : Exchange 2003 SP2, Exchange 2007 SP0/SP1
  - Exploit : cross-site scripting dans OWA (x2)
    - http://blogs.technet.com/swi/archive/2008/07/08/MS08-039-which-users-are-vulnerable-to-OWA-XSS-vulnerability.aspx
  - Crédit : Michael Jordan / Context Information Security

Avis Microsoft (3/15)

- MS08-040 Elévation de privilèges
  - Affecte : SQL Server (toutes versions supportées, y compris "Windows Internal Database")
  - Exploit :
    - Réutilisation de pages mémoire
    - "Buffer overflow" dans la fonction CONVERT
    - Autres corruptions mémoire (x2)
      - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=723
      - Exploitable à l'ouverture d'un fichier de sauvegarde ".MTF"
      - http://blogs.technet.com/swi/archive/2008/07/08/MS08-039-which-users-are-vulnerable-to-OWA-XSS-vulnerability.aspx
  - Crédit :
    - Brett Moore
    - Anonymous (x3)

Avis Microsoft (4/15)

- Correctifs de Août 2008

  - MS08-041 Faille dans un composant ActiveX livré avec Access
    - Affecte : Access 2000 SP3, Access XP SP3, Access 2003 SP2/SP3
    - Exploit : composant "SnapShot Viewer"
      - Exploité "dans la nature"
      - http://blogs.technet.com/swi/archive/2008/08/12/ms08-041-the-microsoft-access-snapshot-viewer-activex-control.aspx
    - Crédit : n/a

  - MS08-042 Faille dans Word
    - Affecte : Word XP SP3, Word 2003 SP2/SP3
    - Exploit : exécution de code à l'ouverture d'un document malformé
      - Exploité "dans la nature"
      - http://blogs.technet.com/swi/archive/2008/08/12/ms08-042-understanding-and-detecting-a-specific-word-vulnerability.aspx
    - Crédit : ISC/SANS

Avis Microsoft (5/15)

- MS08-043 Failles dans Excel (x4)
  - Affecte : Excel (toutes versions supportées) + Excel Viewer + Office 2007 compatibility pack + SharePoint 2007 + Office pour Mac (toutes versions supportées)
  - Exploit :
    - exécution de code à l'ouverture d'un document malformé
    - stockage des identifiants ODBC dans le fichier ".xlsx"
      - http://blogs.technet.com/swi/archive/2008/08/12/ms08-043-how-to-prevent-this-information-disclosure-vulnerability.aspx
  - Crédit :
    - iDefense (x2), ZDI, Jeremy Funk

- MS08-044 Failles dans les convertisseurs Office (x5)
  - Affecte : Works 8, Office 2000 SP3, Office XP SP3, Office 2003 SP2, Project XP SP1, Office converter pack
  - Exploit : exécution de code à l'ouverture d'un fichier malformé
    - EPS, PICT (x2), BMP, WPG
  - Crédit :
    - Shaun Colley / NGS, Damian Put / ZDI, iDefense (x2)

Avis Microsoft (6/15)

- MS08-045 Failles dans IE (x5)
  - Affecte : IE (toutes versions supportées)
  - Exploit : exécution de code à l'ouverture d'un fichier HTML malformé
  - Crédit :
    - Yamata Li (Palo Alto Networks)
    - Tavis Ormandy (Google)
    - Sam Thomas / ZDI
    - ZDI

- MS08-046 Faille dans Windows Color Management
  - Affecte : Windows 2000 / XP / 2003 (toutes versions supportées)
  - Exploit : exécution de code à l'ouverture d'un fichier ICM
  - Crédit : Jun Mao / iDefense

Avis Microsoft (7/15)

- **MS08-047 Problème dans le traitement des stratégies IPSEC**
  - **Affecte : Vista & 2008 (toutes versions supportées)**
  - **Exploit : une stratégie IPSEC exportée depuis Windows 2003 peut ne pas être importée correctement sur Windows 2008**
  - **Crédit : n/d**

- **MS08-048 Faille dans Outlook Express**
  - **Affecte : Outlook Express et Windows Mail (toutes versions supportées)**
  - **Exploit : redirection conservant la zone de confiance via un lien "mhtml://"**
  - **Crédit : Jorge Luis Alvarez Medina / Core**

Avis Microsoft (8/15)

- MS08-049 Failles dans Windows Event System (x2)
  - Affecte : Windows (toutes versions supportées)
  - Exploit : exécution de code via une demande de souscription (requière une authentification)
  - Crédit : Yamata Li / Palo Alto Networks
    - http://blogs.technet.com/swi/archive/2008/08/13/ms08-049-when-kind-of-authentication-is-needed.aspx

- MS08-050 Faille dans Windows Messenger
  - Affecte : Messenger 4.7 et 5.1
  - Exploit : fuite d'information via le contrôle ActiveX "Messenger.UIAutomation.1"
    - http://blogs.technet.com/swi/archive/2008/08/12/ms08-050-locking-an-activex-control-to-specific-applications.aspx
  - Crédit : Haifei Li / Fortinet

Avis Microsoft (9/15)

- **MS08-051 Failles dans PowerPoint (x3)**
  - **Affecte : PowerPoint (toutes versions supportées) + PowerPoint Viewer + Office 2007 compatibility pack + Office 2004 pour Mac**
  - **Exploit : exécution de code à l'ouverture d'un document malformé**
  - **Crédit :**
    - **Ruben Santamarta / Reversemode + iDefense**
    - **ADLab / VenusTech**

Avis Microsoft (10/15)

- Voir également:
  - Mises à jour "non sécurité"
    - http://technet.microsoft.com/en-us/wsus/bb466214.aspx
  - Liste des mises à jour SUS
    - http://support.microsoft.com/kb/894199
  - Dont la mise à jour des "kill bits"
    - http://www.microsoft.com/technet/security/advisory/953839.mspx
    - Nouveaux: Aurigma, HP

- Prévisions pour Septembre 2008
  - 4 bulletins "critiques"
    - Windows Media Player
    - "Microsoft Windows, Internet Explorer, .NET Framework, Office, SQL Server, Visual Studio"
    - Windows Media Encoder
    - Office

Avis Microsoft (11/15)

- Advisories
  - Q951306
    - (Elévation de privilèges locale, exploitable à travers IIS)
    - Mise à jour: Windows XP SP3 est également affecté
  - Q953635
    - Faille dans Word XP SP3 (uniquement)
    - Exploitée dans la nature
    - Corrigé par MS08-042
  - Q954960
    - Le problème de déploiement avec WSUS a été résolu (dans la version 2 du patch :)

Avis Microsoft (12/15)

- Q955179
  - Faille dans le contrôle Access "Snapshot Viewer"
    - Permet de télécharger un fichier à un emplacement de son choix
    - Exploitation via un fichier ".snp"
      - http://research.eeye.com/html/alerts/zeroday/20080707.html
      - http://pstgroup.blogspot.com/2008/07/exploitmicrosoft-office-snapshot-viewer.html
      - http://www.f-secure.com/weblog/archives/SNP.HTML
  - Corrigé par MS08-041
- Q956187
  - Niveau de risque élevé sur la "faille DNS" : publication d'un code d'exploitation fonctionnel

Avis Microsoft (13/15)

- Révisions
  - MS07-047
    - Version 3.0 : Windows XP SP3 est affecté
  - MS07-050
    - Version 2.0 : IE7 sur Windows XP SP3 est affecté
  - MS07-064
    - Version 3.0 : DirectX 9.0a est affecté
  - MS07-068
    - Version 2.2 : Windows Media Runtime 9 + Windows XP SP3 n'est pas affecté
  - MS08-022
    - Version 2.0 : changement de méthode d'installation (permet de contourner les problèmes documentés)
    - Version 2.1 : ajout du suffixe "-v2" aux noms de fichiers
  - MS08-028
    - Version 1.3 : Problème Q950749 résolu
  - MS08-033
    - Version 2.0 : DirectX 9.0a est affecté
    - Version 2.1 : MBSA 2.1a été mis à jour pour détecter ce correctif
  - MS08-037
    - Version 2.0 : Problème avec ZoneAlarm et CheckPoint Integrity
    - Version 2.1 : précisions sur les bulletins remplacés par ce patch (patch cumulatif)
    - Version 2.2 : ajout de 3 problèmes connus dans la FAQ

Avis Microsoft (14/15)

- MS08-039
  - Version 1.1 : information concernant OWA Premium
  - Version 1.2 : Exchange 2000 SP3 n'est pas affecté, mise à jour de la section WSUS
- MS08-040
  - Version 1.1 : SQL Server 2005 SP1 n'est pas affecté
  - Version 1.2 : problèmes connus et documentés
  - Version 1.3 : mise à jour de la section WSUS
  - Version 1.4 : précision sur MSDE 2000
  - Version 1.5 : dans certains cas, la suppression du correctif supprime également la BDD
  - Version 1.6 : changement de la méthode d'installation du correctif
- MS08-043
  - Version 1.1 : mise à jour de la FAQ
  - Version 1.2 : seuls SharePoint 2007 Enterprise et SharePoint 2007 for Internet Sites sont affectés
- MS08-044
  - Version 1.1 : les mises à jour Project 2002 SP1 et Office XP SP3 sont strictement identiques
- MS08-045
  - Version 1.1 : mise à jour des clés de base de registre ; nouveau *workaround* documenté

Avis Microsoft (15/15)

- MS08-047
  - Version 1.1 : Windows XP 64 n'est pas affecté
- MS08-048
  - Version 1.1 : mise à jour de différentes informations techniques
- MS08-051
  - Version 1.1 : mise à jour de la FAQ, Office 2008 pour Mac n'est pas affecté
  - Version 2.0 : le patch pour Office 2003 à télécharger n'était pas complet / la version Office Update était correcte

Infos Microsoft (1/4)

- Sorties logicielles
  - SQL Server 2008
  - Visual Studio 2008 SP1 / .NET 3.5 SP1
  - SoftGrid devient App-V 4.5 RC
  - IE8 Beta2
    - Fonction "InPrivate" ... pour bloquer Google Analytics ?
  - Windows Small Business Server 2008
  - URLScan 3.0 RTM

  - Microsoft lance un site de "social bookmarking" pour Technet
    - http://social.technet.microsoft.com/bookmarks/

  - Hyper-V + Windows Server Core 2008 gratuit d'ici 1 mois !
    - http://www.microsoft.com/servers/hyper-v-server/default.mspx
    - http://www.getvirtualnow.com/

- Mise à jour des politiques de licence et de support
  - Pour inclure la virtualisation (avec Hyper-V)
    - http://www.microsoft.com/licensing/resources/volbrief.mspx
    - http://support.microsoft.com/kb/897615

Infos Microsoft (2/4)

- Midori, le remplaçant de Windows ?
  - Un OS basé sur le noyau Singularity
    - http://www.infoworld.com/article/08/07/29/Microsoft_prepares_for_end_of_Windows_with_Midori_1.html
- Un site consacré au SDL
  - http://www.microsoft.com/sdl/
- "Secure The World" Initiative
  - http://blogs.technet.com/ecostrat/archive/2008/08/06/helping-secure-the-planet-new-strategic-initiatives-from-microsoft.aspx
  - Présentée à BlackHat
    1. Microsoft Vulnerability Research (*failles dans les applications tierce*)
    2. Microsoft Active Protections Program (*pré-notification des bulletins*)
    3. Exploitability Index
- Tout pour être recruté chez Microsoft ☺
  - http://blogs.msdn.com/debuggingtoolbox/archive/2008/07/16/the-microsoft-interview-process-videos-articles-and-material.aspx

Infos Microsoft (3/4)

- Microsoft versera $100,000 par an à la fondation Apache
  - http://arstechnica.com/news.ars/post/20080725-microsoft-to-sponsor-of-the-apache-software-foundation.html
- "Skape" (Matt Miller) embauché chez Microsoft
  - http://blogs.zdnet.com/security/?p=1731
- Après Microsoft Surface, Microsoft Sphere
  - http://research.microsoft.com/~benko/projects/sphere/
- BSOD happens ...
  - http://gizmodo.com/5035456/blue-screen-of-death-strikes-birds-nest-during-opening-ceremonies-torch-lighting

Infos Microsoft (4/4)

Vista

- Le blind test de Vista
  - http://www.mojaveexperiment.com/
- 300 millions de dollars pour relancer Vista
  - http://www.silicon.fr/fr/news/2008/07/25/microsoft___300_millions_de_dollars__pour_retablir_la_verite__sur_vista
- Bill Gates s'y colle
  - http://www.microsoft.com/windows/#
  - http://www.vnunet.fr/news/windows_vista_bill_gates_et_jerry_seinfeld_a_la_rescousse-2028582
- Vista SP1 vs. XP SP3 ... pour les gamers
  - http://www.extremetech.com/article2/0,1558,2302495,00.asp?kc=ETRSS02129TX1K0000532
  - Résultat: égalité ☺

Infos Réseau

- "La" faille DNS ...
  - Tout a déjà été dit ☺
    - http://www.globalsecuritymag.fr/Dan-Kaminsky-IO-Active-Wake-up,20080808,4392
    - (...)
  - La position de l'ICANN sur DNSSEC
    - http://www.icann.org/en/announcements/announcement-24jul08-en.htm
  - Le ".org" va passer à DNSSEC (?)
    - http://arstechnica.com/news.ars/post/20080722-org-first-top-level-domain-to-adopt-dns-security-protocol.html
  - La société de HD Moore victime d'empoisonnement DNS
    - http://www.pcworld.com/article/149126/2008/07/.html
    - http://blogs.zdnet.com/security/?p=1608
  - Patcher BIND en 1 ligne ?
    - http://it.slashdot.org/it/08/08/29/127210.shtml
    - http://www.doxpara.com/?p=1234

Infos Réseau

- BGP: l'autre faille
  - Le nouveau "Big One" ?
    - http://blog.wired.com/27bstroke6/2008/08/revealed-the-in.html
  - Ou un problème connu depuis 10 ans ?
    - http://isc.sans.org/diary.html?storyid=4975
- Clés SSH + "Ring of Trust OpenPGP" = sécurité ?
  - http://web.monkeysphere.info/
- "IPv6 deployment at Google"
  - http://www.ietf.org/proceedings/08jul/slides/plenaryw-4.pdf
- Google lance son propre navigateur: "Chrome"
  - Basé sur WebKit
  - Officiel:
    - http://www.google.com/chrome/
    - http://www.google.com/googlebooks/chrome/

Infos Réseau

- **Non officiel:**
  - **http://arstechnica.com/news.ars/post/20080901-google-opens-up-new-front-in-browser-wars-with-chrome.html**
  - **http://yro.slashdot.org/article.pl?sid=08/09/03/0247205**
  - **http://blogs.codes-sources.com/ebartsoft/archive/2008/09/03/google-chrome-faille-de-s-curit.aspx**
  - **http://aviv.raffon.net/2008/09/03/GoogleMule.aspx**
  - **http://blogs.technet.com/robert_hensing/archive/2008/09/03/on-chromium-and-practical-windows-sandboxing.aspx**
  - **http://blogs.technet.com/robert_hensing/archive/2008/09/03/breaking-out-of-the-chrome-sandbox-2-interesting-vulns-in-24-hours-got-ie8.aspx**
  - **http://www.zdnet.fr/actualites/internet/0,39020774,39383035,00.htm?xtor=RSS-1**
  - **http://www.avertlabs.com/research/blog/index.php/2008/09/04/google-chrome-and-the-404/**
  - **http://flyingoverclouds.spaces.live.com/blog/cns!13F8EFC2E48DC1B3!519.entry**
  - **(...)**

Infos Unix

- Les bugs de sécurité sont-ils des bugs comme les autres ?
  - Linus vs. Pageexec vs. BSD ☺
- La future Debian Stable s'appellera "Squeeze"
- L'infrastructure du projet Fedora compromise
  - Des paquets OpenSSH ont été signés avec la clé Fedora
    - https://www.redhat.com/archives/fedora-announce-list/2008-August/msg00008.html
    - https://www.redhat.com/archives/fedora-announce-list/2008-August/msg00012.html
    - http://rhn.redhat.com/errata/RHSA-2008-0855.html
- Les clés SSH "faibles" (= Debian ☺) largement attaquées "dans la nature"
  - http://it.slashdot.org/it/08/08/27/1413238.shtml
- Linux.exe ... un programme MS-DOS
  - http://www.wolfmountaingroup.org/

Infos Unix

- Nouveautés dans KVM
  - "Nested virtualization"
  - "Memory ballooning"
- Suse 11.1 propose SELinux
  - http://news.opensuse.org/2008/08/20/opensuse-to-add-selinux-basic-enablement-in-111/
  - Le chant du cygne pour AppArmor ?
- Le noyau 2.6.26 supporte le débogage noyau (kgdb) à travers un port série
- WINE passe la 1.0 (après 15 ans de développement)
  - http://www.winehq.org/?announce=1.0
- Linux Symposium 2008
  - http://ols.fedoraproject.org/OLS/Reprints-2008/

Failles

- Produits tiers vulnérables
  - Firefox < 2.0.0.16
  - ThunderBird < 2.0.0.16
  - Firefox < 3.0.1
    - Note: la même faille dans CSSValue affecte les deux versions (ainsi que ThunderBird)
  - Wireshark < 1.0.3
  - Opera < 9.52
  - RealPlayer
    - http://service.real.com/realplayer/security/07252008_player/en/
  - Java (10+ failles)
    - Affecte: Java < 1.6.07, Java < 1.5.16
    - http://secunia.com/advisories/31010/
  - VMWare
    - Affecte: Workstation < 6.0.5, Server < 1.0.7, (...)

Failles

- N.Runs annonce avoir trouvé 800 failles dans des produits antivirus
  - http://blogs.zdnet.com/security/?p=1445
- Faille critique dans Joomla
  - Largement exploitée dans la nature
  - http://developer.joomla.org/security/news/241-20080801-core-password-remind-functionality.html
- Un code d'exploitation pour IOS PPC
  - http://seclists.org/fulldisclosure/2008/Jul/0532.html
- Dans le "Quaterly Patch" d'Oracle ...
  - Une faille PLSQL exploitable via le portail Web
    - http://lists.grok.org.uk/pipermail/full-disclosure/2008-July/063255.html
- Faille dans le parseur PDF de BlackBerry
  - http://isc.sans.org/diary.html?storyid=4733
- Une faille dans le parseur ASN1 du noyau Linux
  - http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-1673
  - Score CVSS : 10/10 ☺

Failles

- OpenSolaris LiveCD "vulnérable par défaut"
  - http://c-skills.blogspot.com/2008/08/opensolaris-remote-root-exploit.html
- Une faille découverte dans YACC
  - Introduite il y a 33 ans ☺
    - http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9108978
- Une faille dans "ed" ☺
  - http://lists.gnu.org/archive/html/bug-ed/2008-06/msg00000.html
- Faille dans l'ActiveX Cisco WebEx
  - http://www.cisco.com/warp/public/707/cisco-sa-20080814-webex.shtml
- Contournement du verrouillage d'écran iPhone
  - http://www.vnunet.fr/news/la_securite_d_acces_a_l_iphone_contournee-2028505
- Les failles dans les CPU, exploitables à distance ?
  - http://blogs.zdnet.com/security/?p=1492
  - http://www.networkworld.com/news/2008/071408-researcher-to-demonstrate-attack-code.html

Malwares et spam

- Un fichier multimédia malicieux
  - Fichier Windows Media "infecté" par un script
  - Utilise la commande "AddScript" pour infecter tous les fichiers locaux
    - http://securitylabs.websense.com/content/Blogs/3145.aspx
- 150 milliards de spams par jour
  - Dont seulement 50% en anglais
  - http://www.vnunet.fr/news/150_milliards_de_spams_par_jour
- Un virus à bord de la station ISS
  - ... à travers une clé USB
  - http://science.slashdot.org/article.pl?sid=08/08/27/1231224
- Casser du CAPTCHA: un business d'avenir
  - $2 les 1000 unités en Inde
    - http://decaptcher.com/
    - http://blogs.zdnet.com/security/?p=1835

Malwares et spam

- Les conclusions du projet "S.P.A.M. Experiment"
  - http://www.mcafee.com/us/research/spam_diaries/index.html
- Un virus déjouant les systèmes de SnapShot "à la SteadyState"
  - http://www.avertlabs.com/research/blog/index.php/2008/07/11/are-internet-cafes-and-bars-in-danger/
- Comment retourner un BotNet
  - http://www.secureworks.com/research/threats/coreflood-removal/
- Un BotHerder relâché en Nouvelle-Zélande
  - 1,000,000 de machines dans le botnet
  - Mais le juge ne voulait pas handicaper l'avenir de l'enfant par une sentence trop lourde ...
    - http://www.nzherald.co.nz/section/1/story.cfm?c_id=1&objectid=10521614

Malwares et spam

- Les antivirus, principale source de failles ?
  - http://www.zdnet.fr/actualites/informatique/0,39040745,39382204,00.htm
- Le "cloud computing" gagne les antivirus
  - Principe : déporter une partie de l'analyse sur le serveur de l'éditeur ...
    - http://www.lesnouvelles.net/articles/technologies/trendmicro-revolution-cloud-computing
    - http://securite.reseaux-telecoms.net/actualites/lire-les-sept-risques-du--cloud-computing-18483.html
- Le "roi du spam" s'évade et tue toute sa famille avant de se suicider
  - http://blogs.zdnet.com/security/?p=1553
  - A noter :
    - *"As part of the restitution, Davis has agreed to forfeit property he purchased, including gold coins (which the IRS is selling today), with the ill gotten proceeds of his offense."*

Malwares et spam

- Un exemple de *vishing* utilisant des messages téléphoniques réels
  - http://isc.sans.org/diary.html?storyid=4951
- Le nombre de machines participant à des *botnets* a quadruplé en 3 mois
  - http://www.shadowserver.org/wiki/pmwiki.php?n=Stats.BotCount90-Days
- Après RBN, Atrivo fait parler de lui
  - http://voices.washingtonpost.com/securityfix/2008/08/report_slams_us_host_as_major.html

Failles 2.0

- Les machines à voter moins fiable que le papier
  - Une étude de Chantal Enguehard, Université de Nantes
- La Géorgie victime de DDoS
  - http://asert.arbornetworks.com/2008/07/georgia-on-my-mind-political-ddos/
  - Presque tout a été dit sur le sujet ...
- Best Western égare 8 millions de numéros de CB
  - Malgré sa certification PCI-DSS
  - http://isc.sans.org/diary.html?storyid=4928
- 41 millions de comptes bancaires compromis par Wardriving
  - http://www.clubic.com/actualite-154738-cyber-fraude-usa.html
- 1 millions de numéros de CB pour £35 ?
  - C'est possible sur eBay !
  - http://fr.news.yahoo.com/grp_test/20080827/ttc-les-coordonnees-bancaires-de-1-milli-549fc7d.html

Failles 2.0

- Facebook ne croit pas aux XSS
  - http://www.theregister.co.uk/2008/08/25/facebook_security_hole/
- Une armée de "hackeuses" Chinoises
  - "Cn Girl Security Team"
  - 2200 membres
  - http://www.asianoffbeat.com/default.asp?Display=1879
- Un conseiller de Gordon Brown se fait voler son BlackBerry par une prostituée chinoise
  - http://www.theregister.co.uk/2008/07/21/government_dataloss_china/
  - http://www.timesonline.co.uk/tol/news/politics/article4364353.ece

Actualité (France)

- Rapport du sénat
  - "Cyberdéfense : un nouvel enjeu de sécurité nationale"
    - http://senat.fr/noticerap/2007/r07-449-notice.html
- La base des clients Dassault Systèmes retrouvée chez Siemens PLM
  - http://www.silicon.fr/fr/news/2008/09/03/dassault_systemes_espionne_par_siemens_plm_software
- Le futur passe Weneo de la SNCF
  - RFID, 4 Go de mémoire, USB, rechargeable à domicile ...
  - http://www.rfidjournal.com/article/articleprint/4283/-1/1/
- Le "paquet télécom" repoussé au 22 septembre
  - http://www.pcinpact.com/actu/news/44839-paquet-telecom-vote-filtrage-amendements.htm
- Des casseurs de DRM relaxés
  - http://www.ecrans.fr/Stop-DRM,4741.html
- Le Conseil d'Etat confirme l'exception pour copie privée
  - http://www.april.org/articles/communiques/pr-20080730.html
- Le projet de loi HADOPI bientôt adopté ?
  - http://www.secuobs.com/news/13082008-hadopi.shtml

Actualité (USA)

- Tout matériel informatique entrant aux USA peut être étudié pendant un temps illimité
  - http://www.journaldunet.com/solutions/breve/juridique/30188/les-etats-unis-autorisent-leurs-douanes-a-fouiller-tout-ordinateur-portable.shtml
- Un administrateur indélicat bloque le réseau de la ville de San Francisco
  - http://www.vnunet.fr/fr/news/2008/07/22/la_municipalite_de_san_francisco_toujours_a_la_porte_de_son_systeme_informatique
  - http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/07/14/BAOS11P1M5.DTL
- La CIA et le FBI lancent le Facebook du renseignement: "A-Space"
  - http://www.zdnet.fr/actualites/internet/0,39020774,39383095,00.htm?xtor=EPR-100
- UAL perd $100m en 1h
  - Sur la base d'une info de ... 2002
  - http://www.forbes.com/home/2008/09/08/ual-tribune-bankruptcy-biz-media-cz_ja_0908ualstory2.html

Actualité

- Google Android
  - Overview
    - http://www.openhandsetalliance.com/android_overview.html
  - Lancement
    - Prévu pour: Octobre 2008
    - Prix: $199
    - Plateforme matérielle : HTC Dream
  - Détails
    - http://news.cnet.com/8301-1035_3-10019041-94.html?hhTest=1
    - http://gizmodo.com/5039741/t+mobile-android-htc-dream-launch-details-oct-13-199-w-2+year-contract-only
    - http://gizmodo.com/5038586/an-in+depth-video-tour-of-android-09-an-almost-great-almost-os
  - SDK
    - http://code.google.com/android/download_list.html
  - Android vs. iPhone
    - http://www.appleinsider.com/articles/08/06/11/google_ceo_occasionally_excused_from_apple_board_meetings.html

Actualité

- Journée contre les brevets logiciels le 24 septembre 2008
  - http://stopsoftwarepatents.org/
- Cuil va-t-il supplanter Google ?
  - http://www.cuil.com/
- Google présente ses méthodes de gestion de la sécurité à la conférence RSA
  - http://www.itnews.com.au/News/73635,google-shares-its-security-secrets.aspx
- Yahoo! coupe la musique
  - Quid des fichiers protégés ?
    - http://www.ecrans.fr/Yahoo-contourne-difficilement-ses,4742.html
- NXP perd son procès contre les "casseurs" du chip Mifare
  - http://www.01net.com/editorial/387107/la-securite-de-millions-de-cartes-a-puce-sans-contact-serieusement-remise-en-question/
- Internet, un immense système de Pay-per-View en 2012 ?
  - http://ipower.ning.com/netneutrality2

Fun

- L'aéroport de Dublin arrêté par une carte réseau
  - http://it.slashdot.org/article.pl?sid=08/07/18/0351231
- Bandai lance le SmartBerry
  - http://www.journaldugeek.com/?2008/07/21/12328-bandai-lance-le-smart-berry
- Le LHC en Open Source
  - http://gizmodo.com/5041973/build-your-own-large-hadron-collider-in-162-x-1028-easy-steps
- De fausses files d'attente pour lancer l'iPhone en Pologne
  - http://actu.voila.fr/Article/mmd--francais--journal_internet--hightech/Des-fausses-files-d-attente-avec-des-figurants-pour-lancer-l-iPhone-en-Pologne.html
- Un PC à $12 ?
  - http://www.zdnet.fr/actualites/informatique/0,39040745,39382652,00.htm
- Les spécialistes "IT Security" moins heureux que la moyenne
  - http://ask.slashdot.org/askslashdot/08/08/24/1731228.shtml

Fun

- Les français font parler d'eux à BlackHat et Defcon
  - Equipe française 2ème au CTF
  - Un compte-rendu décalé ...
    - http://fr.securityvibes.com/blackhat-usa-vegas-debriefing-2008-article-949.html
  - Des "journalistes" de Global Security Mag expulsés
    - http://news.cnet.com/8301-1009_3-10010989-83.html?hhTest=1

Questions / réponses

- Questions / réponses
- Prochaine réunion le mardi 7 octobre 2008
- N'hésitez pas à proposer des sujets et des salles