OSSIR
Groupe Paris

Réunion du 8 septembre 2009

Revue des dernières vulnérabilités

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

Avis Microsoft (1/18)

- **Correctif de Juillet 2009**
  - **Avec [exploitability index]**
  - **(*) = version supportée, à jour des patches**

  - **MS09-028 Failles dans DirectX (x3) [1,1,1]**
    - **Affecte: DirectX 7.0 – 9.0**
    - **Exploit: 3 failles exploitables**
      - **Dont la faille "QuickTime" (quartz.dll) exploitée dans la nature**
    - **Crédit:**
      - **Thomas Garnier / SkyRecon (x2)**
      - **Zheng Wenbin, Liu Qi, and Song Shenlei / Qihoo 360 Security Center**
      - **Yamata Li / Palo Alto Networks (x2)**
      - **Aaron Portnoy / TippingPoint-ZDI**

Avis Microsoft (2/18)

- MS09-029 Failles dans le support des polices "intégrées" (x2) [1,1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: exécution de code à l'ouverture d'un fichier ".eot" malformé
    - Ouverture automatique depuis Internet possible
  - Crédit:
    - Thomas Garnier
    - VeriSign-iDefense
  - http://blogs.technet.com/srd/archive/2009/07/14/ms09-029-vulnerabilities-in-the-eot-parsing-engine.aspx

- MS09-030 Faille dans Publisher [1]
  - Affecte: Publisher 2007 SP1
  - Exploit: fichier ".pub" malformé
  - Crédit:
    - Lionel d'Hauenens / Labo Skopia (via iDefense)

Avis Microsoft (3/18)

- **MS09-031 Faille dans ISA Server 2006 [1]**
  - **Affecte: ISA Server 2006 (SP0 et SP1)**
  - **Exploit: contournement de l'authentification lorsque Radius OTP est utilisé**
  - **Crédit: n/d**
  - **http://blogs.technet.com/isablog/archive/2009/07/13/ms09-031-isa-server-2006-fba-and-radius-otp-bulletin.aspx**

Avis Microsoft (4/18)

- MS09-032 Nouveaux "kill-bits" [1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit:
    - Exécution de code via le contrôle ActiveX "MSVIDCTL.DLL"
    - Exploité dans la nature avant le patch
  - Crédit: Ryan Smith and Alex Wheeler / IBM ISS X-Force

- Ce bogue n'a pas fini de faire parler de lui !

  - Microsoft a-t-il fait "due diligence" ?
    - http://blogs.technet.com/msrc/archive/2009/07/09/questions-about-timing-and-microsoft-security-advisory-972890.aspx

  - La faille dans MSVIDCTL.DLL se situe en fait dans la librairie ATL
    - De nombreuses applications tierce partie sont potentiellement impactées

    - http://addxorrol.blogspot.com/2009/07/poking-around-msvidctldll.html
    - http://voices.washingtonpost.com/securityfix/2009/07/msft_scrambling_to_close_stubb.html
    - http://archives.neohapsis.com/archives/dailydave/2009-q3/0034.html

Avis Microsoft (5/18)

- **MS09-033 Faille dans Virtual PC/Virtual Server [3]**
  - **Affecte: Virtual PC et Virtual Server (toutes versions supportées, sauf Mac OS)**
  - **Exploit: élévation de privilèges dans l'invité**
  - **Crédit: Julien Tinnes et Tavis Ormandy / Google**
  - **http://blogs.technet.com/srd/archive/2009/07/14/ms09-033-the-virtual-pc-vulnerability-is-not-a-vm-breakout-issue.aspx**

Avis Microsoft (6/18)

- Patch(s) "hors bande"
  - MS09-034
    - Affecte: IE (toutes versions supportées)
    - Exploit:
      - Protection "générique" contre la faille ATL
      - Protection contre le contournement du mécanisme de "kill bits"
        - Cf. Black Hat
      - Failles diverses (x3)

Avis Microsoft (7/18)

- MS09-035
  - Affecte:
    - Visual Studio 2003 SP1
    - Redistribuable VS2005 SP1 (973923)
    - Redistribuable VS2008 SP0/SP1 (973924)
    - Visual Studio 2005 SP1 (971090)
    - Visual Studio 2008 SP0/SP1 (971092)
  - Exploit: faille dans la librairie ATL (cf. MS09-032 & Q972260)

- Liste des tiers affectés
  - Java (JRE toutes versions supportées)
    - http://sunsolve.sun.com/search/document.do?assetkey=1-66-264648-1
  - Cisco
    - http://www.cisco.com/warp/public/707/cisco-sa-20090728-activex.shtml
  - Adobe ShockWave
    - http://www.adobe.com/support/security/bulletins/apsb09-11.html

Avis Microsoft (8/18)

- **Correctif de Août 2009**
  - **MS09-036 Déni de service dans ASP.NET [3]**
    - **Affecte: IIS 7.0 (via une faille .NET 2.0 -> .NET 3.5 SP1)**
    - **Exploit: déni de service à distance via une requête HTTP malformée (et non authentifiée)**
      - **Prérequis: le "*worker pool*" IIS doit fonctionner en mode "intégré" et pas en mode "natif"**
      - **http://blogs.technet.com/srd/archive/2009/08/11/ms09-035-asp-net-denial-of-service-vulnerability.aspx**
    - **Crédit: Alexander Pfandt / Digitaria**
  - **MS09-037 Nouvelles failles ATL (x5) [1,1,1,1,1]**
    - **Affecte: Windows (toutes versions supportées sauf Windows 7 / 2008R2)**
      - **Outlook Express, Windows Media Player, éditeur DHTML, MSWebDVD, ...**
    - **Exploit: exécution de code (plusieurs API vulnérables)**
      - **http://blogs.technet.com/srd/archive/2009/08/11/ms09-037-why-we-are-using-cve-s-already-used-in-ms09-035.aspx**
    - **Crédit:**
      - **Ryan Smith & Alex Wheeler / IBM ISS X-Force**
      - **Robert Freeman / IBM ISS X-Force**
      - **David Dewey / IBM ISS X-Force**
      - **Ryan Smith / iDefense (x2)**

Avis Microsoft (9/18)

- MS09-038 Failles Windows Media (x2) [2,2]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: fichier AVI malformé
  - Crédit: Vinay Anantharaman / Adobe (x2) (!)

- MS09-039 Failles WINS (x2) [1,2]
  - Affecte: Windows 2000 Server (*) / Windows 2003 (*)
  - Exploit: requête WINS malformée
    - http://blogs.technet.com/srd/archive/2009/08/11/ms09-039-more-information-about-the-wins-security-bulletin.aspx
  - Crédit:
    - ZDI
    - LiGen / National University of Defense Technology (Chine)

Avis Microsoft (10/18)

- **MS09-040 Faille MSMQ [1]**
  - **Affecte: Windows 2000 (*) / XP SP2 (mais pas SP3) / 2003 (*) / Vista "Gold" (mais pas SP1+)**
  - **Exploit: déréférencement de pointeur NULL dans MQAC.SYS**
  - **Crédit: Nikita Tarakanov / Positive Technologies Research Team (Russie)**

- **MS09-041 Faille dans le service "Workstation" [1]**
  - **Affecte: Windows XP / 2003 / Vista / 2008**
  - **Exploit: "*double free*" dans NetrGetJoinInformation()**
  - **Crédit : Cody Pierce / TippingPoint**

Avis Microsoft (11/18)

- **MS09-042 Faille dans le client Telnet [1]**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit: "*credential reflection*" via le client Telnet**
  - **Crédit: n/d**

- **MS09-043 Failles dans "Office Web Components" (x4) [1,1,1,1]**
  - **Affecte: Office XP, Office 2003, ISA Server, BizTalk ...**
  - **Exploit: failles multiples ("*buffer overflow*", etc.)**
    - **OWC est un contrôle ActiveX**
    - **Au moins une faille exploitée dans la nature avant la disponibilité du correctif**
    - **La faille est connue depuis 2 ans (!)**
  - **Crédit:**
    - **Peter Vreugdenhil / ZDI (x3)**
    - **Haifei Li / Fortinet**
    - **Sean Larsson / iDefense**

Avis Microsoft (12/18)

- **MS09-044 Failles dans RDP (x2) [2,1]**
  - **Affecte: client RDP 5.0 -> 6.1 et client RDP Mac 2.0**
  - **Exploit: "*heap overflow*"**
    - **1 faille dans le client MSTSC**
    - **1 faille dans le contrôle ActiveX "Remote Desktop"**
  - **Crédit:**
    - **Wushi / Team509 + ZDI**
    - **Yamata Li**

Avis Microsoft (13/18)

- Bilan sur la faille "ATL"
  - Points d'entrée
    - http://www.microsoft.com/atl
    - http://msdn.microsoft.com/en-us/visualc/ee309358.aspx
  - Q&A
    - http://blogs.technet.com/msrc/pages/security-bulletin-webcast-q-a-oob-july-2009.aspx
  - Blogs Microsoft
    - http://blogs.msdn.com/sdl/archive/2009/07/28/atl-ms09-035-and-the-sdl.aspx
    - http://blogs.technet.com/srd/archive/2009/07/28/overview-of-the-out-of-band-release.aspx
    - http://blogs.technet.com/srd/archive/2009/07/28/internet-explorer-mitigations-for-atl-data-stream-vulnerabilities.aspx
    - http://blogs.technet.com/srd/archive/2009/07/28/atl-vulnerability-developer-deep-dive.aspx
    - http://blogs.technet.com/srd/archive/2009/07/28/msvidctl-ms09-032-and-the-atl-vulnerability.aspx
  - Blogs tiers
    - http://codetest.verizonbusiness.com/
    - http://hexblog.com/2009/07/casts_are_bad_1.html
    - http://securityblog.verizonbusiness.com/2009/07/28/activex-risk/

Avis Microsoft (14/18)

- 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
- Prévisions pour Septembre 2009
  - 3 bulletins "critiques" affectant:
    - Windows, toutes versions supportées
  - 1 bulletins "critique" affectant:
    - Windows Vista et 2008
  - 1 bulletins "critique" affectant:
    - Windows 2000, XP et 2003

Avis Microsoft (15/18)

- Advisories
  - 967940
    - V1.1: Ajout d'un lien vers le paramètre "HonorAutorunSetting"
  - 971778 -> MS09-028
  - 972890 -> MS09-032
  - 973472 -> MS09-043
    - Affecte: Office XP & 2003, ISA Server 2004 & 2006
    - Exploit: faille dans le contrôle ActiveX "Office Web Components"
      - Exploité dans la nature
      - http://blogs.technet.com/srd/archive/2009/07/13/more-information-about-the-office-web-components-activex-vulnerability.aspx
  - 973811: "Extended Protection for Authentication"
    - Doit être activé globalement dans la base de registre
    - Les applications doivent explicitement demander la protection (IE, Telnet, ...)

Avis Microsoft (16/18)

- 973882: faille dans la librairie ATL
  - Cf. MS09-032, MS09-035, MS09-037
  - V3.0: Windows Live Messenger < 14.0.8089 est également affecté
- 975191: faille(s) dans le FTP intégré à IIS
  - http://blogs.technet.com/srd/archive/2009/09/01/new-vulnerability-in-iis5-and-iis6.aspx
  - V2.0: mise à jour des solutions de contournement
  - Faille #1: affecte IIS 5.0, 5.1 et 6.0
    - Exécution de code possible sur IIS 5.0
  - Faille #2: affecte IIS 5.0, 5.1, 6.0 et 7.0
    - Déni de service, mais tous les processus IIS sont tués
  - Une faille antédiluvienne ?
    - http://research.eeye.com/html/advisories/published/AD19990124.html
- 975497: exécution de code sur Vista / 2008 R1
  - Affecte: SMB 2.0
  - http://archives.neohapsis.com/archives/fulldisclosure/2009-09/0090.html

Avis Microsoft (17/18)

- Révisions
  - MS09-014
    - V1.3: mise à jour d'une "feature key"
  - MS09-016
    - V1.2: problèmes documentés
  - MS09-028
    - V2.0: DirectX 8.1b est aussi affecté
  - MS09-029
    - V1.1: le redémarrage n'est pas toujours obligatoire
    - V2.0: problème d'installation détecté, republication complète du bulletin
    - V2.1: mise à jour de la FAQ
    - V3.0: re-publication du bulletin pour la version Japonaise de Windows
  - MS09-030
    - V1.1: ajout de problèmes connus
  - MS09-032
    - V1.1: mise à jour de la FAQ
    - V1.2: mise à jour de la FAQ
  - MS09-033
    - V1.1: ajout de la ligne de commande pour Vista/2008
  - MS09-034
    - V2.0: problème avec la version coréenne du patch pour IE6 sur Windows 2000

Avis Microsoft (18/18)

- MS09-035
  - V1.1: mise à jour de la FAQ
  - V2.0: prise en compte des "Smart Devices"
  - V2.1: nombreuses corrections documentaires
  - V2.2: comment vérifier la bonne installation du correctif
  - V2.3: mise à jour de la FAQ
- MS09-036
  - V1.1: mise à jour de la FAQ
- MS09-037
  - V1.1: nombreuses corrections documentaires
  - V1.2: précision sur les bulletins remplacés par celui-ci
- MS09-039
  - V1.1: précision sur les bulletins remplacés par celui-ci
- MS09-042
  - V1.1: publication du bulletin (?!?)
- MS09-043
  - V1.1: nombreuses corrections documentaires
- MS09-044
  - V1.1: mise à jour de la FAQ
  - V1.2: correction d'une clé de base de registre
  - V2.0: correction de liens

Infos Microsoft

- **Sorties logicielles**
  - **SilverLight 3**
  - **Windows Seven RTM**
    - **Dans la nature bien avant la disponibilité "officielle" ☺**
      - **http://techwoo.com/windows-7-download/**
  - **Windows 2008 R2 RTM**
  - **WSUS 3.0 SP2**
  - **Exchange 2010 RC**

Infos Microsoft

- **Autre**
  - **Internet Explorer perd du terrain**
    - **http://www.techcrunch.com/2009/07/05/since-march-internet-explorer-lost-114-percent-share-to-firefox-safari-and-chrome/**
  - **IE8 : communication fail ?**
    - **http://www.youtube.com/watch?v=xB9fhjnJcB0**
  - **Microsoft se met d'accord avec l'Europe**
    - **IE8 sera optionnel dans Windows Seven**
      - **http://www.ft.com/cms/s/987b3324-78aa-11de-bb06-00144feabdc0,Authorised=false.html**
  - **Digg (et d'autres acteurs majeurs du Web 2.0) vont-il bloquer IE6 ?**
    - **http://blog.digg.com/?p=878**

Infos Microsoft

- Windows Seven en RTM
  - http://www.youtube.com/watch?v=BQX-y7mtFVg
  - http://winprogger.com/?p=1097
- Windows Seven va-t-il marcher ?
  - Pas sûr ...
    - http://www.solutions-logiciels.com/actualites.php?actu=5459
- Comment on fabrique un Windows Seven ?
  - http://winprogger.com/?p=1097
- "Windows XP Mode" disponible en RC
  - http://windowsteamblog.com/blogs/windows7/archive/2009/08/04/windows-xp-mode-rc-now-available.aspx
  - En conséquence l'activation de la virtualisation matérielle dans les BIOS devient un sujet "chaud"
    - http://www.theregister.co.uk/2009/08/06/sony_vaio_virtualization_disabled/
- Ne manquez pas la soirée de lancement ☺
  - http://fr.houseparty.com/windows7fr

Infos Microsoft

- Microsoft ferme SoapBox et Popfly
  - http://bleucactus.net/2009/07/mashups-microsoft-ferme-popfly/
  - http://www.pcworld.fr/2009/07/24/internet/microsoft-soapbox/437521/
- Bill Gates: "les lois américaines de protection de la vie privée sont trop contraignantes"
  - http://www.nytimes.com/2009/07/25/technology/companies/25soft.htm?_r=1
- Microsoft vs. RealPolitik
  - HideTaiwan()
    - http://msdn.microsoft.com/en-us/library/ms441219.aspx
- Microsoft pose un brevet sur le stockage de documents dans un fichier XML
  - USPTO 7,571,169
- Mais la société canadienne "i4i" avait breveté l'utilisation de XML en 1998
  - Et obtient $200m de Microsoft ...
    - http://blogs.zdnet.com/BTL/?p=22595

Infos Microsoft

- Lancement de Windows MarketPlace
  - Le modèle de "l'Apple Store"
    - http://developer.windowsmobile.com/
- L'API du Windows Security Center expire plus tôt que prévu
    - http://windowsteamblog.com/blogs/windowssecurity/archive/2009/05/06/upcoming-action-center-changes-for-security-vendor-software.aspx
- Comment exploiter plus de 4Go de RAM sur Vista 32 bits
    - http://www.geoffchappell.com/viewer.htm?doc=notes/windows/license/memory.htm
- "You've angered the great Master Russinovich"
    - http://windowsteamblog.com/blogs/springboard/archive/2009/06/22/you-ve-angered-the-great-master-russinovich.aspx
- "Red Hat & Ubuntu sont des concurrents dangereux"
    - http://www.goodgearguide.com.au/article/313782/microsoft_acknowledges_linux_threat_windows_client

Infos Microsoft

- Microsoft et Yahoo! se mettent d'accord
  - http://money.cnn.com/2009/07/29/technology/microsoft_yahoo/index.htm?section=money_latest
- Annonces BlackHat 2009
  - Microsoft Security Update Guide
  - Projet Quant
  - Microsoft Office Visualization Tool
- Microsoft chante les héros de l'Open Source (?!?)
  - http://www.microsoft.com/opensource/heroes/default.mspx
- Communication FAIL
  - http://www.papygeek.com/insolite/le-derapage-de-microsoft-tourne-en-derision/

Infos Microsoft

- (Pour ceux qui ne connaissent pas XKCD.com)

Infos Réseau

- **Principales failles**
  - **Faille BGP dans IOS**
    - **http://www.cisco.com/warp/public/707/cisco-sa-20090729-bgp.shtml**
  - **Déni de service ICMP dans Cisco Firewall Service Module**
    - **http://www.cisco.com/warp/public/707/cisco-sa-20090819-fwsm.shtml**
  - **Déni de service sur BIND**
    - **Affecte < 9.4.3P1, < 9.5.1P3, < 9.6.1P1**
    - **Exploité dans la nature**
      - **https://www.isc.org/node/474**
  - **Déni de service sur SQUID**
    - **Affecte: < 3.0.17, < 3.1.0.12**
      - **http://www.squid-cache.org/Advisories/SQUID-2009_2.txt**
  - **Client ISC DHCP < 4.1.0p1, < 4.0.1p1, < 3.1.2p1**
    - **Note: la branche 2.x n'est plus supportée**
    - **CVE-2009-0692**

Infos Réseau

- Problème courant dans l'implémentation de la signature XML
  - La taille du HMAC est spécifiée par le client
  - Affecte de nombreuses implémentations
    - XML Security Library, produits de la société RSA,Apache, Mono, Sun JVM <= 1.6.14, ...
  - Sounds familiar ?
    - Le même bogue a affecté SNMPv3 ...
- Failles multiples dans ColdFusion et JRun
  - XSS, traversée de répertoires, double encodage, etc.
    - http://www.adobe.com/support/security/bulletins/apsb09-12.html
- Traversée de répertoires dans le serveur Web (+ XSS)
  - Affecte: Cisco Unified CCS
  - Exploit: http://www.cisco.com/warp/public/707/cisco-sa-20090715-uccx.shtml
- Injection de ";" dans le firmware Open Source DD-WRT
  - Bienvenue en 2009 ...
    - http://www.theregister.co.uk/2009/07/21/critical_ddwrt_router_vuln/

Infos Réseau

- A quoi sert Internet la nuit ?
  - http://asert.arbornetworks.com/2009/08/the-internet-after-dark/
  - http://asert.arbornetworks.com/2009/08/the-internet-after-dark-part-ii/
- Quand l'ISP s'arrête ...
  - http://www.computerworld.com.au/article/317356/telstra_internet_outage_points_dns_failure
- Fin du mandat de l'ICANN
  - Au 30 septembre 2009
- Sortie de Nmap 5.0
  - http://nmap.org/5/

Infos Unix

- **(Principales) failles**
  - **Faille #1 dans le noyau Linux (*dev/tun*)**
    - **Exploitable grâce à une optimisation du compilateur**
    - **Et jolie exploitation !**
      - **http://grsecurity.net/~spender/cheddar_bay.tgz**
    - **Du coup d'autres bogues GCC ont été trouvés**
      - **http://permalink.gmane.org/gmane.linux.kernel/868008**
  - **Faille #2 dans le noyau Linux (*do_nanosleep()*)**
    - **Déréférencement de pointeur NULL**
      - **http://xorl.wordpress.com/2009/08/06/linux-kernel-do_nanosleep-null-pointer-dereference/**

Infos Unix

- Faille #3 dans le noyau Linux (*proto_ops*)
  - Déréférencement de pointeur NULL
    - http://blog.cr0.org/2009/08/linux-null-pointer-dereference-due-to.html
  - Affecte Linux 2.4.0 – 2.6.30
  - Code d'exploitation fiable disponible
    - http://grsecurity.net/~spender/wunderbar_emporium.tgz

- Faille #4 dans le noyau Linux
  - Déréférencement de pointeur NULL
  - Déclenchable à distance via un paquet WiFi malformé
    - http://xorl.wordpress.com/2009/08/18/linux-kernel-cfg-802-11-remote-null-pointer-dereference/

Infos Unix

- Faille #5 dans le noyau Linux 2.6 (UDP)
  - Corrigée silencieusement dans la 2.6.19
  - De nombreuses distributions n'avaient pas identifié cette correction comme un problème de sécurité ...
    - http://rhn.redhat.com/errata/RHSA-2009-1222.html
    - http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=1e0c14f49d6b393179f423abbac47f85618d3d46
- Et d'autres encore ...
    - http://lists.debian.org/debian-security-announce/2009/msg00189.html
- Dnsmasq < 2.50
    - http://www.thekelleys.org.uk/dnsmasq/CHANGELOG
- Debian vs. DHCP
  - dhcp3 (3.1.1-6+lenny3) stable-security; urgency=high
  - * Reorder patches to actually apply them
- RedHat vs. PERL
    - http://blog.vipul.net/2008/08/24/redhat-perl-what-a-tragedy/

Infos Unix

- Elévation de privilèges dans pulseaudio
  - http://blog.cr0.org/2009/07/old-school-local-root-vulnerability-in.html
- Apache.org compromis
  - http://blogs.apache.org/infra/entry/apache_org_downtime_initial_report
  - https://blogs.apache.org/infra/entry/apache_org_downtime_report
- Apache mod_proxy
  - http://svn.apache.org/viewvc?view=rev&revision=790587
- Apache 2.2: contournement de l'authentification "Basic" ?
  - Non confirmé et difficile à reproduire
    - http://www.securityfocus.com/bid/35840/info
    - http://seclists.org/nmap-dev/2009/q3/0305.html
    - http://seclists.org/nmap-dev/2009/q3/0385.html
- Ruby On Rails: contournement de l'authentification "Digest"
  - http://weblog.rubyonrails.org/2009/6/3/security-problem-with-authenticate_with_http_digest

Infos Unix

- Wordpress < 2.8.4
  - Les problèmes < 2.8.1 n'ont pas été correctement corrigés
    - http://wordpress.org/development/2009/08/wordpress-2-8-3-security-release/
    - http://wordpress.org/development/2009/08/2-8-4-security-release/
  - Note: Wordpress 2.0.x sera déprécié plus tôt que prévu
    - http://wordpress.org/development/2009/07/the-wordpress-2-0-x-legacy-branch-is-deprecated/
- SPIP < 2.0.9
  - http://www.spip-contrib.net/Alerte-securite-SPIP-nouvelle
- TinyMCE editor (affecte Joomla 1.5.12)
  - http://yehg.net/lab/pr0js/advisories/tinybrowser_1416_multiple_vulnerabilities
  - http://developer.joomla.org/security/news/301-20090722-core-file-upload.html
- Fuite d'information dans Joomla 1.5.x également
  - http://developer.joomla.org/security/news/302-20090722-core-missing-jexec-check.html

Infos Unix

- OpenOffice < 3.1.1
- SquirrelMail a bien été "backdooré"
  - http://sourceforge.net/mailarchive/message.php?msg_name=4A727634.3080008%40squirrelmail.org
- PHP ajoute le support de GOTO
  - http://bugs.php.net/bug.php?id=48669

Infos Unix

- Compress::Raw::Zlib
  - "Off by one" conduisant à un DoS
    - Affecte Amavis, SpamAssassin, etc.
  - Exploité dans la nature par "Trojan.Downloader-71014"

- IO::Socket::SSL ne vérifie pas correctement le titulaire d'un certificat
    - http://cpansearch.perl.org/src/SULLR/IO-Socket-SSL-1.26/Changes

- Déni de service à distance multiples sur Solaris
  - SCTP (CVE-2009-2486)
  - ICMP (CVE-2009-2487)
  - NFSv4 (CVE-2009-2488)

Infos Unix

- Ecrasement de fichiers arbitraires sur AIX 5.3
  - Via les variables d'environnement _LIB_INIT_DBG et _LIB_INIT_DBG_FILE
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=815
- Et un simple "bogue" corrigé dans gethostbyname() sur Linux
  - Impossible d'utiliser ::1 et 127.0.0.1 en même temps
    - http://sourceware.org/bugzilla/show_bug.cgi?id=4980

Infos Unix

- **Autre**
  - **PageExec vs. Linus, ça continue**
    - **http://archives.neohapsis.com/archives/dailydave/2009-q3/0041.html**
    - **http://linuxfr.org/2009/07/24/25761.html**
      - **"Spender : Je sais que cela va probablement énerver certains des lecteurs, mais en ce moment je suis en train d'utiliser Windows 7 RC"**
  - **Alan Cox vs. Linus**
    - **http://lwn.net/Articles/343851/**
  - **Qui contribue à Linux ?**
    - **http://blogs.computerworld.com/14576/who_writes_linux_big_business**
  - **Le mainteneur principal de CentOS disparait sans laisser d'adresse**
    - **http://linux.slashdot.org/story/09/07/30/130249/CentOS-Project-Administrator-Goes-AWOL**

Infos Unix

- Un nouveau scheduler pour Linux
  - ... par Con Kolivas
    - http://linux.slashdot.org/story/09/09/06/0433209/Con-Kolivas-Returns-With-a-Desktop-Oriented-Linux-Scheduler
- Changement de politique pour la distribution Debian "Stable"
  - Une version en début de chaque année "paire"
- "/proc/sys/kernel/modules_disabled" ajouté dans le noyau 2.6.31
- Support du "nested VMX" dans KVM
  - Note: "nested SVM" était déjà supporté
    - http://avikivity.blogspot.com/2009/09/nested-vmx-support-coming-to-kvm.html

Infos Unix

- OpenVAS remplace Nessus dans Debian
  - http://lwn.net/Articles/345532/
- Drupal vers un modèle commercial
  - http://buytaert.net/drupal-trademark-policy-officially-available
- La "carte bleue Linux"
  - http://www.cardpartner.com/app/the-linux-foundation
- Women in Free Software
  - http://www.fsf.org/news/summit-on-women-in-free-software

Infos Unix

- **Sortie de Mac OS X "Snow Leopard"**
  - **Avec cette *release*, Apple affiche des ambitions dans le domaine de la sécurité**
    - **Détecte ... 2 virus par défaut**
    - **La boite de Pandore est-elle ouverte ?**
      - **http://www.avertlabs.com/research/blog/index.php/2009/08/27/is-apple-opening-a-can-of-worms/**
      - **http://blogs.zdnet.com/security/?p=4139**
  - **Snow Leopard réinstalle une version vulnérable de Flash**
    - **http://isc.sans.org/diary.html?storyid=7069**
  - **64 bits FAIL**
    - ***"While Snow Leopard includes both 32-bit and 64-bit kernels, it's possible for a 64-bit capable Mac to boot with the 64-bit kernel only under Mac OS X Server 10.6 - Snow Leopard Server. (...) The 2008 and 2009 iMacs are capable of booting the 64-bit kernel in Snow Leopard Server, but must be placed in that mode by holding down the 6 and 4 keys at startup."***
  - **Comment *crasher* Mac OS X en 1 twit**
    - **http://twitter.com/razvanm/status/3152648774**

Infos Unix

- SCNR

Failles

- **Principales applications**
  - **Safari < 4.0.3**
    - **http://support.apple.com/kb/HT3666 (4.0.2)**
    - **http://support.apple.com/kb/HT3733 (4.0.3)**
  - **Chrome < 2.0.172.37**
    - **http://googlechromereleases.blogspot.com/2009/07/stable-beta-update-bug-fixes.html#links**
  - **Chrome < 2.0.172.43**
    - **Lecture mémoire arbitraire dans le moteur V8**
      - **http://googlechromereleases.blogspot.com/2009/08/stable-update-security-fixes.html**
  - **Opera 9**
    - **Correctif: passer à Opera 10 (!)**
      - **http://www.opera.com/docs/changelogs/windows/1000/**

Failles

- FireFox 3.5.0: première faille critique après quelques jours
  - Note: FF 3.5 a été téléchargé plus d'un milliard de fois
- FireFox: toutes les versions antérieures sont vulnérables
  - FireFox 3.0.13
  - FireFox 3.5.2

- Liste des failles disponibles dans VulnDiscoPack pour CANVAS
  - Notez FreeRadius, MySQL, SAP, Samba, ...
    - http://intevydis.com/vd-list.shtml

Failles

- Thunderbird < 2.0.23
  - Certaines failles ont plus de 6 mois ...
- Java < 1.6.15 (hors faille ATL)
    - http://java.sun.com/javase/6/webnotes/6u15.html
- Failles dans les BIOS Intel
  - Cf. BlackHat 2009 / Joanna Rutkowska
    - http://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00018&languageid=en-fr
- Faille dans "Autonomy KeyView"
  - Affecte Lotus Notes, Symantec Antivirus ... et probablement bien d'autres !
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=823

Failles

- Attaque "0day" contre Flash Player et Acrobat Reader
  - Flash Player < 9.0.246.0, < 10.0.32.18
  - Acrobat Reader < 9.1.3
    - http://www.adobe.com/support/security/bulletins/apsb09-10.html
  - Note: Acrobat Reader embarque un lecteur Flash depuis la version 9 ...
    - http://www.adobe.com/support/security/advisories/apsa09-03.html
    - http://blogs.adobe.com/psirt/2009/07/potential_adobe_reader_and_fla.html
    - http://secer.org/tech/new-0-day-attacks-using-pdf-documents.html
  - Mais visiblement tout le monde ne croit pas au danger des failles ☺
    - http://www.acrobatusers.com/articles/why-javascript-acrobat

Failles

- iPhone < 3.0.1
  - Faille "SMS" révélée à BlackHat
    - http://support.apple.com/kb/HT3754
- Mac OS X < 10.5.8
    - http://support.apple.com/kb/HT3757
- VLC < 1.0.1
- Wireshark < 1.2.1
- ActiveX "Akamai Download Manager"
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=813

Failles

- Correctifs Oracle du mois de juillet
  - (Au moins) 29 failles corrigées
    - http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2009.html
- Faille(s) à venir sur les *parsers* XML
    - http://www.cert.fi/en/reports/2009/vulnerability2009085.html
    - http://www.codenomicon.com/news/press-releases/2009-08-05.shtml
- WPA/TKIP cassé à nouveau ? Ou pas ...
  - La mise en œuvre de l'attaque nécessite un MiTM radio
    - http://jwis2009.nsysu.edu.tw/index.php/jwis/jwis2009/paper/view/80

Failles 2.0

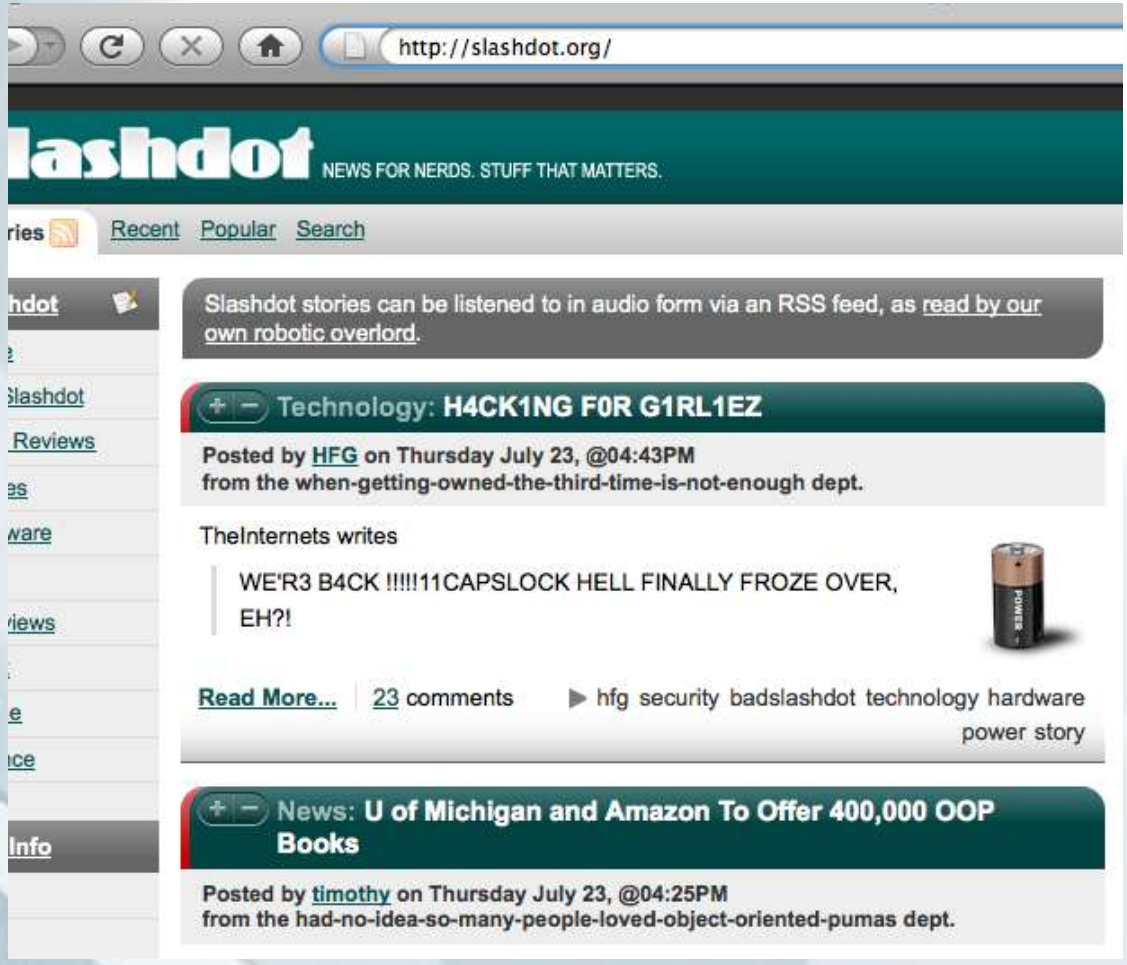
- Comment Twitter a failli disparaitre ...
  - http://www.korben.info/hack-de-twitter-la-suite.html
- Twitter filtre les domaines malveillants
  - Sur la base de Google API
    - http://www.f-secure.com/weblog/archives/00001745.html
- Twitter, Facebook (et d'autres) sous attaque DoS
  - http://status.twitter.com/post/157191978/ongoing-denial-of-service-attack

Failles 2.0

- Un DoS affectant tous les navigateurs existants
  - <script>select(2^31)</script>
    - http://www.g-sec.lu/one-bug-to-rule-them-all.html
- Network Solutions laisse fuiter une bonne partie de sa base client
  - Incluant les numéros de CB
    - http://about.networksolutions.com/site/data-security-alert-problem-fix-and-customers-notified/
- "Pretty Bad Proxies" vs. SSL
    - http://research.microsoft.com/apps/pubs/default.aspx?id=79323
- Le site des Nations Unies vulnérable depuis 2 ans
  - Une leçon en gestion des risques
    - http://erratasec.blogspot.com/2009/08/uns-website-still-vulnerable-after-2.html

Failles 2.0

- Slashdot (Europe ?) compromis



Malwares et spam

- McAfee vs. Tavis Ormandy
  - http://my.opera.com/taviso/blog/month-of-mcafee-bugs
- Le virus Koobface ajoute le support Twitter
  - http://www.avertlabs.com/research/blog/index.php/2009/07/13/koobface-worm-turns-toward-twitter/
- Un ver Symbian se propageant par SMS "texte"
  - En fait un lien vers un ".sis" malveillant hébergé sur le Web
    - http://www.f-secure.com/weblog/archives/00001732.html
- Clampi: le plus gros aspirateur bancaire de tous les temps
  - Plus de 4500 sites visés
    - http://www.cio.com/article/498530/Clampi_Trojan_Revealed_As_Financial_Plundering_Botnet_Monster

Malwares et spam

- 52% des malwares ne sont pas diffusés plus d'une journée
  - http://www.theregister.co.uk/2009/08/13/malware_arms_race/
- Une technique de persistance originale
  - http://www.sophos.com/blogs/sophoslabs/v/post/4380
- Le forum "r00t-y0u" saisi par la police
- IEEE Industry Connections Security Group
  - Premier groupe de travail: Malware Working Group
    - http://grouper.ieee.org/groups/malware/malwg
- Communication fail(ures)
  - http://itvigilante.sophos.fr/
  - http://www.youtube.com/watch?v=kbRSQVsOX_Y

Malwares et spam

- La carte des PC sur lesquels il manque au moins une mise à jour
  - En moyenne 4 applications non patchées
  - Basée sur les données Secunia PSI
    - http://secunia.com/vulnerability_scanning/personal/worldmap/?view=,insecure
- 90% des PC en entreprise ne sont pas à jour
  - Source: Sophos
    - http://www.sophos.com/blogs/gc/g/2009/06/02/ten-work-pcs-fail-basic-security/
- 80% des PC ont une version Flash ou Acrobat vulnérable
    - http://blogs.zdnet.com/security/?p=4097
- Sophos rachète Utimaco (?)
    - http://www.securityvibes.com/sophos-utimaco-jsaiz-news-935.html

Actualité (France)

- L'ANSSI officiellement créée
  - http://www.pcinpact.com/actu/news/51844-anssi-securite-attaques-informatique-agence.htm?vc=1
- Les PME françaises de plus en plus espionnées
  - D'après la DCRI
    - http://www.mag-securs.com/spip.php?article13871
- Les pannes informatiques se multiplient au PMU
  - Même sans attaques ...
    - http://cheval.blog.lemonde.fr/2009/08/12/big-bug-au-pmu-l%E2%80%99usine-a-gaz-au-bord-de-l%E2%80%99implosion/
- Zataz retourne devant la justice
  - http://www.zataz.com/news/19391/jugement--zataz.html

Actualité (France)

- Travailler pour HADOPI et mourir
  - http://www.korben.info/bougez-avec-hadopi-big-brother-a-enfin-un-nom.html
  - http://www.korben.info/extelia-hadopi.html
- ODEBI lance un projet d'armée numérique
  - http://www.numerama.com/magazine/13492-La-Ligue-ODEBI-lance-un-projet-d-armee-numerique.html
- Alain Juillet part dans un cabinet d'avocats américain
  - http://www.letelegramme.com/ig/generales/france-monde/france/alain-juillet-passe-a-l-ennemi-30-08-2009-528515.php
- Google numérisera le fond de la BnF
  - Et cela fait grincer des dents
    - http://passouline.blog.lemonde.fr/2009/08/25/la-colere-de-jeanneney-contre-laccord-google-bnf/

Actualité (France)

- Les français ont les pires politiques de mots de passe en Europe
  - 1 seul mot de passe pour tous les sites !
    - http://www.20minutes.fr/article/345357/High-Tech-Les-Francais-cancres-des-mots-de-passe.php

- Enfin ... surtout les hommes ☺
  - 47% hommes vs. 26% femmes
    - http://tempsreel.nouvelobs.com/depeches/medias/multimedia/20090904.ZDN0240/les_femmes_plus_prudentes_que_les_hommes_sur_internet_.html

Actualité (anglo-saxonne)

- BlackHat 2009 & Defcon 17
  - Voir CR précédent ☺
  - Les agences gouvernementales s'inquiètent du nombre de badges RFID qui ont pu être "scannés"
    - http://www.wired.com/threatlevel/2009/08/fed-rfid/
- Un DDoS contre des sites gouvernementaux américains
  - On peut difficilement parler de "cyberguerre"
    - http://blogs.csoonline.com/online_attack_hits_us_government_web_sites
  - Origine: Corée du Nord ?
    - http://fr.news.yahoo.com/3/20090709/twl-usa-internet-attaques-informatiques-224d7fb.html
- Un concours pour recruter 10,000 cyber-experts
    - http://www.internetnews.com/security/article.php/3823806/Feds+Need+10000+Cyber+Security+Experts.htm

Actualité (anglo-saxonne)

- Conserver les compétences, un vrai problème pour l'état américain
  - http://politics.theatlantic.com/2009/08/when_john_brennan_the_presidents.php
- L'envoi d'un mail cause la panique
  - Message légitime, mais contenant les données de 27,000 employés de l'état américain
    - http://www.washingtonpost.com/wp-dyn/content/article/2009/08/03/AR2009080302013.html
- La fraude s'étend
  - L'auteur de plusieurs intrusions dans des systèmes de paiement aurait eu accès à 130 millions de comptes au total
    - http://www.lefigaro.fr/international/2009/08/18/01003-20090818ARTFIG00195-fraude-record-a-la-carte-bancaire-aux-etats-unis-.php
- Gary McKinnon va finalement être extradé vers les USA
  - http://news.bbc.co.uk/2/hi/uk_news/8177561.stm

Actualité (anglo-saxonne)

- L'échec de PCI/DSS analysé par Heartland Payment Systems
  - http://www.csoonline.com/article/499527/Heartland_CEO_on_Data_Breach_QSAs_Let_Us_Down
- "L'affaire" Amazon/Kindle donne un aperçu du futur numérique
  - http://www.slate.com/id/2223214/
- ATT bloque "4chan"
  - Un autre aperçu du futur ?
    - http://www.techcrunch.com/2009/07/26/att-blocks-4chan-this-is-going-to-get-ugly/
  - Des attaques "plus intelligentes que la moyenne" ont immédiatement eu lieu
    - http://digg.com/tech_news/AT_T_CEO_Dead_outside_his_home_iReport_com?OTC-kff

Actualité (Google)

- Les Google Apps ne sont plus en Beta !
  - http://googleblog.blogspot.com/2009/07/google-apps-is-out-of-beta-yes-really.html
- Google Apps Script est disponible
  - Dans la version payante
    - http://googleenterprise.blogspot.com/2009/08/launched-google-apps-script.html
- Google annonce Chrome OS
  - http://googleblog.blogspot.com/2009/07/introducing-google-chrome-os.html
- Les résultats du concours "Google Native Client" publiés
  - Les français sont classés ☺
    - http://googlecode.blogspot.com/2009/07/native-client-security-contest-results.html

Actualité (Google)

- La ville de Los Angeles passe tout son SI chez Google
  - Une fausse bonne idée ?
    - http://blog.emagined.com/2009/07/21/trouble-brewing-in-the-cloud/
- Google Maps attaqué en justice par Bottin.fr
  - Demande 500,000 euros de dommages et intérêts
    - http://www.zdnet.fr/actualites/internet/0,39020774,39703340,00.htm
- La Défense bientôt sur Google Street View
    - http://www.monputeaux.com/2009/08/des-tricyles-google-sur-le-parvis-de-la-d%C3%A9fense.html
- Google pose un brevet sur sa page d'accueil
    - http://yro.slashdot.org/story/09/09/03/1223207/Google-Patents-Its-Home-Page

Actualité (Google)

- Google Chrome
  - Chrome pour Linux (en beta, bien sûr)
    - http://dev.chromium.org/getting-involved/dev-channel
  - The Courgette Updating System ☺
    - http://dev.chromium.org/developers/design-documents/software-updates-courgette
  - Communication Google Chrome
    - http://www.youtube.com/watch?v=6OAGLm_BQyI
  - Un *easter egg* dans Chrome x64 fait fantasmer
    - http://code.google.com/p/chromium/issues/detail?id=18385

Actualité (Google)

- Le métier de Google expliqué par son patron
  - http://standblog.org/blog/post/2009/08/17/Le-m%C3%A9tier-de-Google%2C-expliqu%C3%A9-par-son-patron
- La femme du fondateur de Google a aussi des idées ...
  - L'analyse génétique pour tous !
    - https://www.23andme.com/
- Google UK prend feu
  - A la suite d'un BBQ ...
    - http://www.telegraph.co.uk/technology/google/6099593/Fire-breaks-at-out-Google-building-in-Victoria-London.html
- Google WIN ☺
  - http://www.google.com/search?q=ascii+art
- Google FAIL ☺
  - http://www.google.fr/search?q=999999999999999+-+999999999999998

Actualité

- Le monde libre est sous attaque
  - Parmi les victimes récentes:
    - ImageShack
    - Matasano
      - http://seclists.org/fulldisclosure/2009/Jul/0388.html
    - Kevin Mitnick, Dan Kaminsky, Julien Tinnes, ...
      - Cf. "zf05.txt"
    - darkmindz, elitehackers, hak5, binrev, blackhat-forums, ...
  - "Antisec" devient un nom du domaine public ...
    - http://romeo.copyandpaste.info/
  - En tout cas Open0wn fait parler de lui ☺
    - http://lwn.net/Articles/340483/

Actualité

- Le W3C renonce à standardiser les balises <audio> et <video>
  - Sous la pression d'Apple
    - http://www.lemondeinformatique.fr/actualites/lire-le-w3c-renonce-a-specifier-les-balises-audio-et-video-dans-html-5-28863.html
- Str0ke arrête milw0rm (?)
    - http://milw0rm.com/
- L'opérateur télécom des Emirats Arabes Unis décide de backdoorer les BlackBerry
  - Seul problème: ça n'était pas très subtil
    - http://www.theregister.co.uk/2009/07/14/blackberry_snooping/
- Quand le contrôle parental dérape
    - http://www.google.com/hostednews/ap/article/ALeqM5i5CjgMEdrwRm3JxeglUykMAHAYmAD9AGNVM00
- Quand le pentest dérape
    - http://isc.sans.org/diary.html?storyid=7024

Actualité

- Dans les écoles de hacking chinoises
  - Attention: article de propagande
  - Mais quand même 1 million d'inscrits sur le forum ...
    - http://www.chine-informations.com/actualite/enquete-dans-les-ecoles-de-hacking-en-chine_13472.html
- 1 professionnel de la sécurité sur 2 n'est pas content de son boulot
    - http://www.darkreading.com/security/management/showArticle.jhtml?articleID=218600434
- "48% des PDG pensent que les piratages de réseau d'entreprise par des hackers restent du domaine anecdotique"
    - http://www.lemondeinformatique.fr/actualites/lire-les-ceo-sous-estiment-les-risques-informatiques-28907.html
- Une base de données privée contenant 40 millions de comptes bancaires volés
  - En faites-vous partie ?
    - https://www.lucidintelligence.com/

Actualité (crypto)

- Un chip quantique réussit à multiplier 3 et 5
  - Prêt pour la production de masse
    - http://www.newscientist.com/article/dn17736-codebreaking-quantum-algorithm-run-on-a-silicon-chip.html
- Perte du HSM => perte de la CA => FAIL
  - A priori un équivalent allemand de la Carte Vitale
    - http://www.h-online.com/security/Loss-of-data-has-serious-consequences-for-German-electronic-health-card--/news/113740
- Vulnérabilités dans les TPM ... à vendre !
    - http://seclists.org/fulldisclosure/2009/Jul/0414.html
- Casser SHA1/MD5 sur cartes ATI
  - Gratuit et très rapide !
    - http://golubev.com/hashgpu.htm

Actualité (crypto)

- L'autre projet NaCl
  - Une librairie cryptographique optimisée
    - http://nacl.cace-project.eu/
- $250,000 pour cracker Nagra3
    - http://hardware.slashdot.org/story/09/07/16/1913227/Three-Arrested-For-Conspiring-To-Violate-the-DMCA
- Attaque impressionnante sur AES
  - Mais des conditions de mise en œuvre rarement vérifiées en pratique
    - http://www.schneier.com/blog/archives/2009/07/another_new_aes.html

Fun

- La compatibilité peut faire gagner de l'argent
  - http://my.opera.com/hallvors/blog/2009/07/20/most-expensive-javascript-ever
- La migration vers FireFox 3 victime de contraintes imprévues
  - http://www.pcpro.co.uk/blogs/2009/08/26/porn-collection-put-people-off-upgrading-to-firefox-3/
- Challenge Defcon par l'image
  - http://hackerschool.org/DefconCTF/17/B300.html
- Un message chiffré cassé 2 siècles plus tard
  - http://online.wsj.com/article/SB124648494429082661.html
- Nabaztag en faillite ☹
  - http://savenabaztag.com/
  - Des idées pour le relancer ?
  - http://www.freeangel.fr/

Fun

- La clé RSA-512 de la TI-83+ factorisée
  - http://permalink.gmane.org/gmane.comp.encryption.general/13439
- Microsoft parraine un "FireFox"
  - http://www.korben.info/microsoft-finance-firefox.html
- $5000 si vous arrivez à localiser ce journaliste pendant ses vacances
  - http://www.wired.com/vanish/2009/08/author-evan-ratliff-is-on-the-lam-locate-him-and-win-5000/
- La disparition d'un prototype d'iPhone conduit au suicide d'un employé
  - http://digital.venturebeat.com/2009/07/21/iphone-prototype-goes-missing-chinese-worker-investigated-commits-suicide/
- What else ?
  - http://www.newlisp.org/

Fun

- Le premier appareil photo "Open Source" ...
  - http://news.stanford.edu/news/2009/august31/levoy-opensource-camera-090109.html

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 13 octobre 2009
- N'hésitez pas à proposer des sujets et des salles