OSSIR
Groupe Paris

Réunion du 14 septembre 2010

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Juillet 2010**
  - **Références**
    - **http://blogs.technet.com/b/msrc/archive/2010/07/13/july-2010-security-bulletin-release.aspx**
    - **http://blogs.technet.com/b/msrc/p/july-2010-security-bulletin-q-a.aspx**
  - **MS10-042 Faille dans "Help and Support Center"[1]**
    - **Affecte: Windows XP / 2003 (toutes versions supportées)**
    - **Exploit: exécution de commandes à l'ouverture d'une URL**
      - **Exploité dans la nature avant la publication du correctif**
      - **http://blogs.technet.com/b/srd/archive/2010/07/13/ms10-042-vulnerability-in-help-and-support-center.aspx**
    - **Crédit: n/a**
      - **Publié de manière "irresponsable" par Tavis Ormandy ☺**

Avis Microsoft

- **MS10-043 Faille dans "Canonical Display Driver" [2]**
  - **Affecte: Windows 7 / 2008 R2 (x64 uniquement)**
  - **Exploit: *integer overflow* (en mode noyau) lors d'un rendu graphique**
  - **Crédit: David Hansel / Reactive Systems**

- **MS10-044 Faille(s) dans un contrôle ActiveX livré avec Access [1,1]**
  - **Affecte: Access 2003 / 2007 (toutes versions supportées)**
  - **Exploit: utilisation de variables non initialisées (conduisant à l'exécution de code)**
    - **http://www.zerodayinitiative.com/advisories/ZDI-10-117/**
  - **Crédit:**
    - **Anonymous / ZDI**
    - **Robert Freeman / IBM ISS X-Force**

Avis Microsoft

- MS10-045 Faille dans Outlook [1]
  - Affecte: Office XP / 2003 / 2007 (toutes versions supportées)
  - Exploit: exécution de code à l'ouverture d'une pièce jointe
    - Via un lien de type "\\serveur\pièce jointe.exe"
    - http://archives.neohapsis.com/archives/fulldisclosure/2010-07/0211.html
    - http://blogs.technet.com/b/srd/archive/2010/07/13/ms10-045-microsoft-office-outlook-remote-code-execution-vulnerability.aspx
  - Crédit: Yorick Koster / SSD SecuriTeam

Avis Microsoft

- **Correctif "hors cycle"**
  - **MS10-046 Faille dans le support des fichiers "LNK"**
    - **Affecte: Windows (toutes versions supportées)**
    - **Exploit: exécution de code lors de l'affichage d'une icône de raccourci**
      - **Très fiable (chargement d'une DLL)**
      - **Largement exploité dans la nature avant la disponibilité du correctif (Q2286198)**
    - **Crédit:**
      - **Sergey I. Ulasen & Oleg Kupreev / VirusBlokAda**
      - **Andreas Marx & Maik Morgenstern / AV-Test**
      - **Will Dormann / CERT/CC**
      - **Niels Teusink**
      - **Stefan Kanthak**
    - **Notes:**
      - **Q&A**
        - **http://blogs.technet.com/b/msrc/p/august-2010-oob-security-bulletin-q-a.aspx**
      - **Des modifications fonctionnelles ont également été apportées**
        - **http://cert.lexsi.com/weblog/index.php/2010/08/06/391-comment-microsoft-a-corrige-la-vulnerabilite-lnk-mais-pas-uniquement**
      - **Ce correctif peut s'installer sur XP SP2 (sans support officiel)**
        - **http://www.f-secure.com/weblog/archives/00002005.html**

Avis Microsoft

- **Août 2010**
  - **Le plus gros "*Patch Tuesday*" de tous les temps**
    - **14 bulletins, 34 failles**
  - **Références**
    - **http://blogs.technet.com/b/msrc/archive/2010/08/10/august-2010-security-bulletin-release.aspx**
    - **http://blogs.technet.com/b/msrc/archive/2010/08/12/august-2010-webcast-and-qa.aspx**
    - **http://blogs.technet.com/b/srd/archive/2010/08/10/assessing-the-risk-of-the-august-security-updates.aspx**
  - **MS10-047 Failles dans le noyau Windows [1,2,?]**
    - **Affecte: Windows (toutes versions supportées sauf Windows 2003)**
    - **Exploit: élévation de privilèges**
    - **Crédit:**
      - **Tavis Ormandy / Google (x3)**

Avis Microsoft

- MS10-048 Failles dans Win32k.sys [?,1,1,1,1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: élévation de privilèges
    - http://www.coresecurity.com/content/microsoft-windows-createwindow-function-callback-bug
    - http://blogs.technet.com/b/srd/archive/2010/08/10/ms10-048-an-explanation-of-the-defense-in-depth-fixes.aspx
    - http://blogs.msdn.com/b/david_leblanc/archive/2010/08/10/ms10-048-getting-the-math-right.aspx
  - Crédit:
    - Tavis Ormandy / Google
    - Matthieu Suiche / Moonsols (x3)
    - Nicolas Economou / Core SDI
  - Note:
    - L'une des failles avait été identifiée comme un *crash* il y a plus de 3 ans
      - http://social.msdn.microsoft.com/Forums/en-US/windowsgeneraldevelopmentissues/thread/57c3783b-dd38-4a57-9217-61a920541ad0

Avis Microsoft

- MS10-049 Failles dans SChannel [3,2]
  - Affecte: Windows (toutes versions supportées)
  - Exploit:
    - "La" faille de renégociation TLS
      - Il est nécessaire de positionner une clé de base de registre
      - http://blogs.technet.com/b/srd/archive/2010/08/10/ms10-049-an-inside-look-at-cve-2009-3555-the-tls-renegotiation-vulnerability.aspx
    - Exécution de code côté client à l'aide d'une réponse malformée
      - http://blogs.technet.com/b/srd/archive/2010/08/10/ms10-049-a-remote-code-execution-vulnerability-in-schannel-cve-2010-2566.aspx
  - Crédit:
    - Marsh Ray & Steve Dispensa / PhoneFactor

Avis Microsoft

- MS10-050 Faille dans Windows Movie maker [1]
  - Affecte: Windows XP & Vista
    - Movie Maker 2.1, 2.6 et 6.0
  - Exploit: exécution de code à l'ouverture d'un fichier projet malformé
    - http://secunia.com/secunia_research/2010-66/
  - Crédit: Dyon Balding / Secunia

- MS10-051 Faille dans MS-XML [2]
  - Affecte: Windows (toutes versions supportées)
    - MS-XML 3.0
  - Exploit: exécution de code lors du traitement d'une réponse AJAX malformée
    - http://code.google.com/p/skylined/issues/detail?id=17
  - Crédit: SkyLined / Google

Avis Microsoft

- MS10-052 Faille dans le codec MP3 [1]
  - Affecte: Windows XP & 2003
  - Exploit: exécution de code à la lecture d'un flux MP3 malformé
    - ZDI-10-147
  - Crédit: Moritz Jodeit / n.runs + ZDI

- MS10-053 Correctif cumulatif pour IE [3,2,1,2,2,1]
  - Affecte: IE (toutes versions supportées)
  - Exploit:
    - Exécution de code à l'ouverture d'une page Web malveillante
    - Contournement des zones de sécurité
  - Crédit:
    - David Bloom / Google
    - Nicolas Joly / VUPEN (x4)
    - Gambino ZaDarkSide

Avis Microsoft

- MS10-054 Faille dans le serveur SMB [2,3,3]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: exécution de code et dénis de service dans le serveur SMB
    - http://archives.neohapsis.com/archives/fulldisclosure/2010-08/0123.html
    - http://blogs.technet.com/b/srd/archive/2010/08/10/ms10-054-exploitability-details-for-the-smb-server-update.aspx
  - Crédit:
    - Laurent Gaffié / Stratsec
    - Todd Wease & Richard Johnson / SourceFire
    - Riku Hietamaki & Joshua Morin / Codenomicon

- MS10-055 Faille dans le codec Cinepak [1]
  - Affecte: Windows XP & Vista & Seven
  - Exploit: exécution de code à l'ouverture d'un flux Cinepak malformé
    - ZDI-10-148
  - Crédit: anonymous / ZDI

Avis Microsoft

- MS10-056 Failles dans Word [1,1,2,2]
  - Affecte: Word (toutes versions supportées sauf Office 2010)
    - Y compris les versions Works 9, Mac, Converter et Viewer
  - Exploit: exécution de code à l'ouverture d'un document Word malformé
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=876
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=877
    - ZDI-10-150, ZDI-10-151
    - http://archives.neohapsis.com/archives/fulldisclosure/2010-08/0126.html
  - Crédit:
    - L.W.Z / team509 + ZDI
    - Wushi / team509 + iDefense
    - team509 + iDefense
    - Rodrigo Rubira Branco / CheckPoint Research
    - Anonymous / ZDI

- MS10-057 Faille dans Excel [1]
  - Affecte: Excel XP & 2003 & Mac
  - Exploit: exécution de code à l'ouverture d'un document Excel malformé
    - http://www.coresecurity.com/content/CORE-2010-0407-Excel-PivotTable-CDR-overflow
  - Crédit: Damian Frizza / Core SDI

Avis Microsoft

- MS10-058 Failles dans le support TCP/IP [3,1]
  - Affecte: Windows Vista & 2008 & Seven & R2
  - Exploit: déni de service distant *ou* élévation de privilèges locale
    - http://moonsols.com/blog/14-august-security-bulletin
  - Crédit:
    - Darren Willis / Fourteenforty Research
    - Matthieu Suiche / MoonSols

- MS10-059 Failles dans "Tracing Feature for Services" [?,1]
  - Affecte: Windows Vista & 2008 & Seven & R2
  - Exploit:
    - ACL incorrecte sur une clé de base de registre, permettant l'élévation de privilèges
      - HKLM\Software\Microsoft\Tracing*
    - Exécution de code à la lecture d'une clé de base de registre malformée
  - Crédit: Cesar Cerrudo / Argeniss (x2)

Avis Microsoft

- MS10-060 Failles .Net [1,1]
  - Affecte: Windows (toutes versions supportées)
    - Compte-tenu du fait que les Framework 2.0 et 3.5 sont installés par défaut
    - Affecte également SilverLight 2.0 et 3.0
  - Exploit: élévation de privilèges
    - Corruption mémoire
    - Erreur de traitement des "Virtual Method Delegates"
    - Exploitable possible via SilverLight ou ASP.NET
  - Crédit:
    - Carsten Book / Mozilla
    - Eamon Nerbonne

Avis Microsoft

- Advisories
  - Q977377 Renégociation TLS/SSL
    - V2.0: publication du correctif
  - Q2219475 Faille dans "Help and Support Center"
    - V2.0: publication du correctif
  - Q2028859 Faille dans "Canonical Display Driver"
    - V2.0: publication du correctif
  - Q2264072 Elévation de privilèges entre un compte de service et le compte SYSTEM
    - Cf. Cesar Cerrudo, BlackHat USA 2010
    - Correctif (partiel) à télécharger manuellement
      - Modifie les ACL sur une clé utilisée par le service TAPI
      - http://support.microsoft.com/kb/982316

Avis Microsoft

- Q2286198 Faille dans le support des fichiers LNK
  - V1.0: publication de l'avis
  - V1.1: mises à jour documentaires
  - V1.2: mises à jour documentaires
  - V2.0: publication du correctif

- Quelques informations pêchées sur Internet
  - Principe
    - Le chargement d'une icône de raccourci fait appel à LoadLibrary()
    - ... donc du code est exécuté
  - La faille peut être exploitée au travers des vecteurs suivants:
    - Fichiers LNK et PIF
    - Liens à l'intérieur d'un document bureautique
  - Détails d'exploitation
    - Un chemin complet vers la ressource (DLL) doit être fourni
    - Le chargement à distance est possible via WebDAV
  - Historique
    - MS05-049
    - http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-12/att-0008/I2S-LAB-10-15-03.Shell32-Do.txt

Avis Microsoft

- Divers
  - Faille "0day" utilisée "dans la nature" (virus "Stuxnet") pour attaquer un système SCADA (Siemens SIMATIC WinCC)
  - L'attaque exploite un login/mot de passe "en dur" dans la base de données
    - http://it.slashdot.org/comments.pl?sid=1721020&cid=32920758
  - Il est impossible de changer ce mot de passe
    - http://www.pcworld.com/businesscenter/article/201442/after_worm_siemens_says_dont_change_passwords.html
  - Le code d'exploitation d'origine contourne UAC
  - Les pilotes malveillants ont été signés avec les clés des sociétés Realtek et JMicron
    - Les deux sociétés sont basées à Taiwan (Hsinchu Science Park)
- Références
  - Code d'exploitation
    - http://www.ivanlef0u.tuxfamily.org/?p=411
  - Protection non officielle
    - http://blog.didierstevens.com/programs/ariad/

Avis Microsoft

- **Q2269637 "*DLL Preloading*"**
  - **V1.0: publication de l'avis**
  - **V1.1: publication d'un "*Fix It*"**
  - **Principe**
    - **Lorsqu'un utilisateur clique sur un fichier, le logiciel associé est lancé automatiquement**
    - **Ce logiciel peut être amené à charger des DLL depuis le répertoire du fichier**
    - **Dangereux dans le cas de clés USB ou de partages réseau**
  - **Références**
    - **http://blogs.technet.com/b/msrc/archive/2010/08/21/microsoft-security-advisory-2269637-released.aspx**
    - **http://blogs.technet.com/b/msrc/archive/2010/08/31/update-on-security-advisory-2269673.aspx**
    - **http://blogs.technet.com/b/srd/archive/2010/08/23/more-information-about-dll-preloading-remote-attack-vector.aspx**
    - **http://blogs.technet.com/b/srd/archive/2010/08/31/an-update-on-the-dll-preloading-remote-attack-vector.aspx**
    - **http://blogs.msdn.com/b/david_leblanc/archive/2010/08/23/another-technique-for-fixing-dll-preloading-attacks.aspx**

Avis Microsoft

- Une technique ancienne …
  - Première référence: Georgi Guninski (2000)
    - http://www.securityfocus.com/bid/1699
  - … d'où l'introduction des clés "SafeDllSearchMode" et "KnownDLLs"
- … relancée par une "faille" iTunes
  - http://www.securityfocus.com/archive/1/513190
- … ainsi que des études récentes
  - http://www.cs.ucdavis.edu/research/tech-reports/2010/CSE-2010-2.pdf
- Exploitation
  - A distance via Chrome
    - http://raffon.net/research/chrome/dllh/game.html
  - Ou plein d'autres
    - http://secunia.com/advisories/windows_insecure_library_loading/
    - http://www.attackvector.org/new-dll-hijacking-exploits-many/
- Détection via Metasploit
  - http://blog.metasploit.com/2010/08/exploiting-dll-hijacking-flaws.html

Avis Microsoft

- Préconisations
  - Tous les logiciels tiers doivent être corrigés …
  - Un *workaround* a été mis à disposition par Microsoft
    - Désactivation du chargement de DLL depuis un emplacement distant
- Note
  - Le problème est connu sous Linux
    - "." dans PATH, LD_*, DT_RUNPATH, etc.
  - … mais pas toujours corrigé ☺
    - http://www.nth-dimension.org.uk/blog.php?id=87

Avis Microsoft

- **Révisions**
  - **MS09-014**
    - **V1.4: correction d'une clé de BdR**
  - **MS10-016**
    - **V2.3: Windows Movie Maker 2.6 n'est pas disponible sur Windows Seven**
  - **MS10-021**
    - **V1.1: changement de la logique de détection**
  - **MS10-024**
    - **V2.0: nouveau bulletin corrigeant le problème KB976323**
      - **Perte de la configuration SMTP sur IIS + Windows 2008**
  - **MS10-041**
    - **V1.4: changement de la logique de détection**
  - **MS10-043**
    - **V1.1: information pour les utilisateurs de Windows 7 / 2008 R2"SP1 Beta"**
  - **MS10-044**
    - **V1.1: documentation du problème KB982335**
  - **MS10-045**
    - **V1.1: documentation du problème KB978212**
  - **MS10-046**
    - **V1.1: mise à jour de la FAQ**
    - **V1.2: changement de l'algorithme de détection**

Avis Microsoft

- MS10-049
  - V1.1: correction de la liste des bulletins remplacés
- MS10-050
  - V1.1: ajout d'un problème connu
- MS10-054
  - V1.1: correction de l'impact
  - V1.2: pas de *fix-it* pour l'une des attaques
- MS10-056
  - V1.1: mise à jour des noms de fichiers
  - V1.2: ajout d'un problème connu
  - V1.3: un correctif additionnel doit être installé pour Word 2007
- MS10-057
  - V1.1: ajout d'un problème connu
- MS10-058
  - V1.1: ajout d'un *workaround*
- MS10-060
  - V1.1: ajout d'un problème connu, mise à jour des *workarounds*

Infos Microsoft

- **Sorties logicielles**
  - **EMET 2.0**
    - **http://blogs.technet.com/b/srd/archive/2010/09/02/enhanced-mitigation-experience-toolkit-emet-v2-0-0.aspx**
  - **Windows Intune (Beta2)**
    - **Fusion de l'informatique interne et du "Cloud"**
      - **http://technet.microsoft.com/en-us/windows/ff472080.aspx**
  - **Le SP1 pour Windows 7 / 2008R2 repoussé à 2011**
    - **Intègrera RemoteFX (entre autres)**
  - **Exchange 2007 SP3**
  - **Exchange 2010 SP1**
  - **Première beta pour IE9 le 15 septembre 2010**

Infos Microsoft

- Microsoft WebMatrix
  - Le EasyPHP de l'ASP.NET ☺
    - http://www.microsoft.com/web/webmatrix/
- Microsoft LightSwitch
  - Visual Studio pour les managers
    - http://www.microsoft.com/visualstudio/en-us/lightswitch
- Déboguer une machine virtuelle Hyper-V depuis l'hôte
  - Un outil publié par Matthieu Suiche (MoonSols)
    - http://moonsols.com/blog/15-livecloudkd-debugging-the-clouds-from-the-moon

Infos Microsoft

- **Autre**
  - Encore un trimestre de bénéfices "record" chez Microsoft
  - "Information Sharing and MSRC 2010"
    - http://www.microsoft.com/downloads/details.aspx?FamilyID=9954af26-046b-48e9-bb40-b3612665fb51&displaylang=en
  - Un espion russe arrêté chez Microsoft
    - http://www.cbsnews.com/8301-501465_162-20010495-501465.html
  - Microsoft Security Essentials reçoit 2 certifications
    - AV-Test.org
      - http://windowsteamblog.com/windows/b/windowssecurity/archive/2010/08/18/microsoft-security-essentials-receives-av-test-certificate.aspx
    - VB100
      - http://windowsteamblog.com/windows/b/windowssecurity/archive/2010/08/12/microsoft-security-essentials-earns-august-vb100-certification.aspx

Infos Microsoft

- Elévation de privilèges locale non corrigée ("0day")
  - Source:
    - http://www.ragestorm.net/blogs/?p=255
  - Réponse:
    - http://blogs.technet.com/b/msrc/archive/2010/08/10/update-on-the-publicly-disclosed-win32k-sys-eop-vulnerability.aspx
- ASP.NET "cassé"
  - Un gros potentiel de destruction
    - http://netifera.com/research/
- Attaque "*pass the ticket*" contre Kerberos
    - http://secgroup.ext.dsi.unive.it/kerberos/
- Publication d'un nouvel exploit pour MS09-050
    - http://www.piotrbania.com/all/smb2_exploit_mirrors.txt

Infos Microsoft

- "Responsible Disclosure" vs. "Full Disclosure"
  - Microsoft parle désormais de "Coordinated Vendor Disclosure"
    - http://blogs.technet.com/b/msrc/archive/2010/07/22/announcing-coordinated-vulnerability-disclosure.aspx
    - http://blogs.technet.com/b/ecostrat/archive/2010/07/22/coordinated-vulnerability-disclosure-bringing-balance-to-the-force.aspx
- A savoir également
  - ZDI va publier ses failles au bout de 6 mois
    - Un moyen de mettre la pression sur les éditeurs
    - http://www.zdnet.com/blog/security/new-vulnerability-disclosure-deadline-puts-pressure-on-tardy-software-vendors/7044

Infos Réseau

- **(Principales) faille(s)**
  - **BIND < 9.7.1-P2**
    - **Annule un changement sur le traitement des enregistrements RRSIG (introduit dans la version 9.7.1)**
      - **http://www.isc.org/software/bind/advisories/cve-2010-0213**
  - **Struts2 / Xwork < 2.2.0**
    - **Exécution de *commandes***
      - **http://blog.o0o.nu/2010/07/cve-2010-1870-struts2xwork-remote.html**
  - **Bogofilter < 1.2.2**
    - ***Heap overflow* dans le décodeur Base64**
      - **http://bogofilter.sourceforge.net/security/bogofilter-SA-2010-01**
  - **phpMyAdmin**
      - **http://www.phpmyadmin.net/home_page/security/PMASA-2010-6.php**
      - **http://www.phpmyadmin.net/home_page/security/PMASA-2010-7.php**

Infos Réseau

- Adobe ColdFusion 8.x et 9.x
  - Traversée de répertoire
    - http://www.adobe.com/support/security/bulletins/apsb10-18.html
  - Conduisant à la compromission complète du serveur
    - http://www.gnucitizen.org/blog/coldfusion-directory-traversal-faq-cve-2010-2861/
- StrongSwan
  - *Buffer overflow*
    - http://download.strongswan.org/patches/08_snprintf_patch/
- Quagga < 0.99.17
    - http://www.quagga.net/news2.php?y=2010&m=8&d=19
- Squid < 3.1.7
    - http://www.squid-cache.org/Versions/v3/3.1/changesets/SQUID_3_1_7.html
- Squid < 3.1.8
    - http://www.squid-cache.org/Advisories/SQUID-2010_3.txt

Infos Réseau

- Cisco IOS 15.1(2)T
  - Déni de service sur TCP (épuisement de ressources)
    - http://www.cisco.com/warp/public/707/cisco-sa-20100812-tcp.shtml
- Cisco IOS-XR
  - Déni de service via BGP
    - http://www.cisco.com/warp/public/707/cisco-sa-20100827-bgp.shtml
  - Note: ce bug a été découvert lors d'une expérimentation "grandeur nature" du RIPE
    - Pour tester une version "sécurisée" de BGP
- Cisco WCS < 6.0.196.0
  - Injection SQL (!)
    - http://www.cisco.com/warp/public/707/cisco-sa-20100811-wcs.shtml
- Cisco WLC
  - "Déni de service", élévation de privilèges, contournement des contrôles d'accès, …
    - http://cisco.com/warp/public/707/cisco-sa-20100908-wlc.shtml

Infos Réseau

- Cisco ASA
  - Failles multiples (TLS, SIP, IKE, SunRPC)
    - http://www.cisco.com/warp/public/707/cisco-sa-20100804-asa.shtml
- Cisco Firewall Services Module
  - Faille dans le support SunRPC
    - http://www.cisco.com/warp/public/707/cisco-sa-20100804-fwsm.shtml
- Cisco ACE
  - Failles multiples (RTSP, HTTP, RTSP, SIP, SSL)
    - http://www.cisco.com/warp/public/707/cisco-sa-20100811-ace.shtml

Infos Réseau

- Cisco UCCX
  - Traversée de répertoire …
    - http://www.cisco.com/warp/public/707/cisco-sa-20100609-uccx.shtml
- Cisco CUCM
  - Déni(s) de service SIP
    - http://www.cisco.com/warp/public/707/cisco-sa-20100825-cucm.shtml
- Cisco CUP
  - Déni(s) de service SIP
    - http://www.cisco.com/warp/public/707/cisco-sa-20100825-cup.shtml
- Cisco WebEx Player
  - http://www.zerodayinitiative.com/advisories/ZDI-10-155/
  - Le correctif a été poussé en avril dernier (!)

Infos Réseau

- Autres infos
  - Ca y est, la zone racine de l'Internet est signée (DNSSEC)
    - http://article.gmane.org/gmane.ietf.general/41065
  - SPIP FAIL
    - http://www.spip.net/fr_article5248.html
  - Qui utilise "mod_status", en vrai ?
    - http://sota.gen.nz/status/
  - Contournement des IDS
    - En émettant des paquets TCP avec un *checksum* invalide
      - http://www.packetstan.com/2010/07/potential-evasion-where-ips-fails-to.html
  - "DNS Made Easy" victime de DDOS
    - http://twitter.com/DNSMadeEasy

Infos Unix

- **(Principales) faille(s)**
  - **X11 vers "*root*"**
    - **http://theinvisiblethings.blogspot.com/2010/08/skeletons-hidden-in-linux-closet.html**
    - **http://lwn.net/Articles/400746/**
  - **FreeBSD 7.1, 7.3 et 8.0**
    - **Elévation de privilèges locale**
      - **http://security.freebsd.org/advisories/FreeBSD-SA-10:07.mbuf.asc**
  - **BSD 7.x et 8.x**
    - **Elévation de privilèges locale (0day)**
      - **http://seclists.org/fulldisclosure/2010/Aug/219**
  - **AIX <= 5.3 (ftpd)**
    - ***Buffer overflow* dans la commande NLST**

Infos Unix

- Faille dans le support CIFS
  - Où est l'avis de sécurité ?
    - http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=4c0c03ca54f72fdd5912516ad0a23ec5cf01bda7
- Pointeur NULL dans le noyau
  - Affecte keyctl_session_to_parent()
    - https://bugzilla.redhat.com/show_bug.cgi?id=627440
  - Crédit: Tavis Ormandy
- OpenLDAP < 2.4.23
  - Exécution de code à distance (avant authentification)
    - http://www.openldap.org/its/index.cgi/Software%20Bugs?id=6570
- MySQL < 5.1.49, < 5.5.5
    - http://dev.mysql.com/doc/refman/5.1/en/news-5-1-49.html
    - http://dev.mysql.com/doc/refman/5.1/en/news-5-1-50.html
    - http://dev.mysql.com/doc/refman/5.5/en/news-5-5-5.html
- 74 (!) failles corrigées dans HP Insight Manager
    - http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-317/CERTA-2010-AVI-317.html

Infos Unix

- JBoss Enterprise 5.0.2
  - Quelques dizaines de bogues corrigés
    - http://www.redhat.com/docs/en-US/JBoss_Enterprise_BRMS_Platform/5.0.2/html/Release_Notes/index.html
- Typo3
  - Failles multiples, dont injection SQL
    - http://typo3.org/teams/security/security-bulletins/typo3-sa-2010-012
- Drupal 5.x et 6.x
    - http://drupal.org/node/880476
- PHPMyAdmin
    - http://www.phpmyadmin.net/home_page/security/PMASA-2010-4.php
    - http://www.phpmyadmin.net/home_page/security/PMASA-2010-5.php
- vBulletin 3.8.6 (uniquement)
  - Le moteur de recherche intégré indexe tous les mots de passe du site
    - FAIL ☺
    - http://www.securityfocus.com/archive/1/512575

Infos Unix

- GPGSM < 2.0.17
  - *Heap overflow*
    - http://lists.gnupg.org/pipermail/gnupg-announce/2010q3/000302.html
- Wget (!)
  - Le serveur peut spécifier un emplacement d'écriture à l'aide de l'entête "Location:"
    - http://www.debian.org/security/2010/dsa-2088
- Lynx 2.x (!!)
  - *Buffer overflow* dans le traitement d'une URL trop longue contenant le caractère"%"
    - https://bugs.launchpad.net/ubuntu/+source/lynx-cur/+bug/613254
- XSS dans Nessus Server ☺
    - https://discussions.nessus.org/message/7245#7245

Infos Unix

- Autre
  - OpenSolaris, c'est fini
    - Il faudra passer à Solaris 11 "Express"
      - http://mail.opensolaris.org/pipermail/opensolaris-discuss/2010-August/059310.html
  - Debian 6.0 (Squeeze)
    - http://www.debian.org/News/2010/20100806
  - AppArmor intégré au noyau 2.6.36
    - http://lkml.org/lkml/2010/7/30/61
  - FreeBSD 8.1

Failles

- **Principales applications**
  - **FireFox < 3.6.7**
    - **http://www.mozilla.org/security/known-vulnerabilities/firefox36.html#firefox3.6.7**
    - **Voir également: ZDI-10-130, ZDI-10-131, ZDI-10-132, ZDI-10-133, ZDI-10-134,**
  - **FireFox < 3.6.8 (une seule faille)**
    - **http://www.mozilla.org/security/known-vulnerabilities/firefox36.html#firefox3.6.8**
    - **http://www.mozilla.org/security/announce/2010/mfsa2010-48.html**
  - **FireFox < 3.6.9**
    - **http://www.mozilla.org/security/known-vulnerabilities/firefox36.html#firefox3.6.9**
  - **ThunderBird < 3.1.1**
    - **http://www.mozilla.org/security/known-vulnerabilities/thunderbird31.html#thunderbird3.1.1**
  - **Pas de correctifs de sécurité dans la version 3.1.2**
    - **http://www.mozillamessaging.com/en-US/thunderbird/3.1.2/releasenotes/**
  - **ThunderBird < 3.1.3**
    - **http://www.mozilla.org/security/known-vulnerabilities/thunderbird31.html#thunderbird3.1.3**

Failles

- Google Chrome < 5.0.375.127
  - http://googlechromereleases.blogspot.com/2010/07/stable-channel-update_26.html
  - http://googlechromereleases.blogspot.com/2010/08/stable-channel-update_19.html
  - La version 5.0.375.126 met à jour le plugin Flash intégré
    - http://googlechromereleases.blogspot.com/2010/08/stable-channel-update.html
- Google Chrome 6.0.472.53 est sorti
  - http://googlechromereleases.blogspot.com/2010/09/stable-and-beta-channel-updates.html
  - Déjà une mise à jour vers 6.0.472.55
    - http://googlechromereleases.blogspot.com/2010/09/stable-beta-channel-updates.html

Failles

- Safari < 4.0.5, iOS < 4.0
  - ZDI-10-152
- Safari < 4.1, < 5.0
    - http://support.apple.com/kb/HT4196
  - ZDI-10-154
- Safari < 4.1.1, < 5.0.1
    - http://support.apple.com/kb/HT4276
  - ZDI-10-141, ZDI-10-142, ZDI-10-144, ZDI-10-153
  - Corrige également l'*autofill*
    - http://jeremiahgrossman.blogspot.com/2010/07/i-know-who-your-name-where-you-work-and.html
- Safari < 4.1.2, < 5.0.2
    - http://support.apple.com/kb/HT4333
  - Corrige la faille "*DLL preloading*"
  - Safari supporte désormais les extensions
    - http://extensions.apple.com/

Failles

- iTunes < 9.2.1
  - Exécution de code via un lien"itpc://"malformé
    - http://support.apple.com/kb/HT4263
- QuickTime < 7.6.7
    - http://support.apple.com/kb/HT4290

- Faille "0day" dans QuickTime
  - ZDI-10-168 (Juin 2010)
  - Redécouverte par Ruben Santamarta
  - Liée à une fonction proche de la "backdoor"
    - http://www.reversemode.com/index.php?option=com_content&task=view&id=69&Itemid=1

- Note: iTunes + QuickTime 10 est sorti
  - Des failles corrigées dans le moteur WebKit
    - http://support.apple.com/kb/HT4328
  - Incluant le réseau social d'Apple: "Ping"
  - … mais sans Facebook (finalement)

- RealPlayer
    - http://service.real.com/realplayer/security/08262010_player/en/

Failles

- Opera < 10.61
  - http://www.opera.com/support/kb/view/966/
  - http://www.opera.com/support/kb/view/967/
  - http://www.opera.com/support/kb/view/968/
  - http://www.opera.com/docs/changelogs/windows/1061/
  - http://secunia.com/secunia_research/2010-110/
- Opera < 10.62
  - Corrige le "*DLL Preloading*"
    - http://www.opera.com/docs/changelogs/windows/1062/
- VLC < 1.1.3
  - http://www.videolan.org/security/sa1004.html
- VLC < 1.1.4
  - Corrige le "*DLL Preloading*"
    - http://www.videolan.org/security/sa1005.html

Failles

- WireShark < 1.2.10
  - http://www.wireshark.org/security/wnpa-sec-2010-07.html
  - http://www.wireshark.org/security/wnpa-sec-2010-08.html
  - WireShark 1.2.11 corrige le "*DLL Preloading*"
    - http://www.wireshark.org/security/wnpa-sec-2010-10.html
  - WireShark 1.4.0 est sorti
- Java (version IBM) < 1.6.0_20
  - http://www.ibm.com/developerworks/java/jdk/alerts/
- Java < 1.6.0_21
  - Pas de faille de sécurité corrigée
    - http://www.oracle.com/technetwork/java/javase/bugfixes6u21-156339.html
  - Supporte désormais Chrome 4.0 & d'autres …
    - http://www.oracle.com/technetwork/java/javase/6u21-156341.html

Failles

- iOS < 4.0.2
  - Faille(s) "0day" exploitée(s) par le site http://jailbreakme.com/
    - Pour "*jailbreaker*" toutes les versions d'iOS connues
      - http://community.websense.com/blogs/securitylabs/archive/2010/08/06/technical-analysis-on-iphone-jailbreaking.aspx
  - Une première faille dans le support des PDF
    - Affecte FreeType < 2.4.2
      - Support du "Compact Font Format"
      - http://www.vupen.com/english/advisories/2010/2018
    - … et donc tous les produits basés sur cette librairie
      - http://freetype.sourceforge.net/index2.html#release-freetype-2.4.2
    - … comme FoxIt Reader < 4.1.1.0805
      - http://www.foxitsoftware.com/announcements/2010861227.html
    - Utilisation massive de "*Return Oriented Programming*" pour l'exploitation
  - Une deuxième faille noyau pour élever ses privilèges
  - Patch disponible quelques jours après
    - http://support.apple.com/kb/HT4291
  - Et code source de l'attaque publié dans la foulée
    - http://github.com/comex/star

Failles

- iOS < 4.1
  - http://support.apple.com/kb/HT4334
  - Note: iOS 4.1 "jailbreaké" en 24h …
    - http://www.theregister.co.uk/2010/09/09/ios_4_dot_1_jailbreak/
- Mac OS X (10.5 et 10.6)
  - http://support.apple.com/kb/HT4312
- Adobe Flash Player < 10.1.82.76
  - http://www.adobe.com/support/security/bulletins/apsb10-16.html
  - Crédits:
    - Will Dormann / CERT
    - Damian Put (ZDI-10-149)
    - Lenovo Security Beijing
    - Jöran Benker
  - Une nouvelle faille détectée en "0day" dans la nature
    - http://www.adobe.com/support/security/advisories/apsa10-03.html

Failles

- Adobe Reader < 8.2.4, < 9.3.4
  - Faille publiée par Charlie Miller lors de sa conférence BlackHat
    - Sans coordination avec Adobe
    - Deux failles affectant OpenOffice ont également été publiées
      - http://securityevaluators.com/files/papers/CrashAnalysis.pdf
  - Corrigée le 19 août 2010
    - http://www.adobe.com/support/security/bulletins/apsb10-17.html
  - Crédit:
    - Tavis Ormandy / Google

Failles

- Adobe Reader
  - Une nouvelle faille détectée en "0day" dans la nature
    - http://contagiodump.blogspot.com/2010/09/cve-david-leadbetters-one-point-lesson.html
    - http://www.adobe.com/support/security/advisories/apsa10-02.html
    - Le code d'exploitation contourne DEP et ASLR sur toutes les plateformes Windows
      - Les attaquants sont compétents ☺

Failles

- Adobe ShockWave < 11.5.8.612
  - http://www.adobe.com/support/security/bulletins/apsb10-20.html
  - Références:
    - TPTI-10-09, TPTI-10-10, TPTI-10-11, TPTI-10-12, TPTI-10-13, TPTI-10-14, TPTI-10-15
    - ZDI-10-160, ZDI-10-161, ZDI-10-162, ZDI-10-163, ZDI-10-164
  - Crédits:
    - Honggang Ren / Fortinet (x3)
    - Aaron Portnoy & Logan Brown / TippingPoint FuzzBox (x3)
    - Aaron Portnoy & Logan Brown & Team lollersk8erz (x3)
    - Aaron Portnoy & Logan Brown & Team Montreal Hotties (x1)
    - Rodrigo Rubira Branco / Check Point (x6)
    - Damian Put / ZDI (x2)
    - Anonymous / ZDI (x3)
    - Anonymous / iDefense (x1)

Failles

- Autonomy KeyView (round #1)
  - Multiples failles trouvées par Secunia Research
    - http://secunia.com/secunia_research/2010-16/
    - http://secunia.com/secunia_research/2010-23/
    - http://secunia.com/secunia_research/2010-27/
    - http://secunia.com/secunia_research/2010-28/
    - http://secunia.com/secunia_research/2010-31/
    - http://secunia.com/secunia_research/2010-35/
    - http://secunia.com/secunia_research/2010-49/
  - Affecte par rebond Lotus Notes, BlackBerry Server, Symantec Antivirus, etc.
    - http://www-01.ibm.com/support/docview.wss?uid=swg21440812
    - http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=2010&suid=20100727_01

- Autonomy KeyView (round #2)
  - ZDI-10-156
  - ZDI-10-157
  - ZDI-10-158
  - ZDI-10-159

Failles

- Akamai Download Manager
  - Faille de type "*download and execute*"
    - http://www.akitasecurity.nl/advisory.php?id=AK20090402
  - Utilisé par de nombreux tiers
    - Microsoft, Adobe, Citrix, McAfee, Symantec …
- Plugin Citrix et clients ICA
    - http://support.citrix.com/article/CTX125975
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=875
- Jetty (serveur Web)
  - Directory traversal et XSS
  - Affectant VMWare vCenter
    - http://www.vmware.com/security/advisories/VMSA-2010-0012.html

Failles

- IBM SolidDB
  - Exécution de code à distance (via le port TCP/1315)
    - http://www.zerodayinitiative.com/advisories/ZDI-10-125/
  - Affecte par rebond des produits tiers
    - Ex. Cisco WCS ?
- EMC Celerra (NAS)
  - / est exporté en NFS
    - http://archives.neohapsis.com/archives/fulldisclosure/2010-08/0018.html
- Elévation de privilèges locale
  - ... via la librairie mathématique fournie par Intel
    - http://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00025&languageid=en-fr

Failles

- Les prix s'envolent
  - $3,000 chez Mozilla
    - http://www.mozilla.org/security/bug-bounty.html
  - $3,133.7 chez Google
    - http://blog.chromium.org/2010/07/celebrating-six-months-of-chromium.html
  - ($0 chez Microsoft)

- Le nombre de failles explose
  - Surtout dans les produits tiers
    - … c'est-à-dire non Microsoft (environ 4 fois plus de failles)
    - http://secunia.com/gfx/pdf/Secunia_Half_Year_Report_2010.pdf

- Metasploit retrouve une GUI
  - ... en Java
    - http://pauldotcom.com/2010/07/metasploit-new-gui.html

Failles

- La prochaine version d'Adobe Reader inclura un"mode protégé"
  - Un bac à sable (de type MOICE ou Chrome)
    - http://blogs.adobe.com/asset/2010/07/introducing-adobe-reader-protected-mode.html
- Adobe rejoint le programme MAPP
    - http://blogs.technet.com/b/msrc/archive/2010/07/28/community-based-defense-looking-outward-moving-forward.aspx

Failles

- "Month of Abysssec Undisclosed Bugs" (MoAUB)
  - http://archives.neohapsis.com/archives/fulldisclosure/2010-09/0003.html
  - cPanel
    - http://www.exploit-db.com/moaub-1-cpanel-php-restriction-bypass-vulnerability/
  - Et plein d'autres
    - QuickTime, Trend Micro ActiveX, HP OpenView, etc.

Failles 2.0

- Cloutage.org
  - Le "hall of shame" du Cloud
    - http://cloutage.org/
- Faille dans Firefox et Chrome
  - *Race condition* sur un *popup* de confirmation
    - http://lcamtuf.coredump.cx/ffgeo2/
  - Exploitable efficacement avec le bogue de "*DLL Preloading*"
- La FIFA "perd" la base des inscrits à la coupe du monde 2006
  - Monnayée €600,000 …
    - http://soccerlens.com/investigators-reveal-massive-world-cup-data-breach/54099/
    - http://www.ico.gov.uk/news/current_topics/wc2006_ticket_disclosure.aspx
- "J'ai archivé FaceBook"
  - 100% légal: seuls les profils publiquement accessibles ont été copiés
    - http://www.thinq.co.uk/2010/7/28/100-million-facebook-pages-leaked-torrent-site/

Failles 2.0

- Twitter arrête l'authentification "*Basic*" pour les applications tierce partie
  - Migration vers OAuth
    - http://www.webmonkey.com/2010/08/twitter-moves-to-oauth-the-oauthcalypse-is-nigh/
- Le mode de navigation "privé" dans les navigateurs
  - … ne serait pas si "privé"
    - http://crypto.stanford.edu/~dabo/pubs/abstracts/privatebrowsing.html

Malwares et spam

- Intel rachète McAfee
  - Plus de 7 milliards de dollars
- Plusieurs personnes impliquées dans le botnet "Mariposa" arrêtées
  - http://www.fbi.gov/pressrel/pressrel10/mariposa072810.htm
- La valse des applications malveillantes
  - Papiers peints sur Android
  - Application dissimulant une fonction de "tethering" sur iPhone
    - "Handy Light"
    - … et son auteur a 15 ans
- Une extension FireFox "backdoorée"
  - "Sniffer": un module destiné aux "pentesteurs"
  - ... qui envoyait tous les mots de passe chez l'éditeur
    - http://news.netcraft.com/archives/2010/07/15/firefox-security-test-add-on-was-backdoored.html
    - http://blog.mozilla.com/addons/2010/07/13/add-on-security-announcement/

Malwares et spam

- Le firmware du serveur PowerEdge R410 contient un virus
  - Dans la carte de *management* intégrée
    - http://en.community.dell.com/support-forums/servers/f/956/t/19339458.aspx
- Un binaire "setuid" en écoute sur le port TCP/12345 des téléphones HTC Evo et HTC Hero
  - Appelons ça un "bogue"…
    - http://www.unrevoked.com/rootwiki/doku.php/public/unrevoked1_disclosure
- Le "Nigerian Scam" rapporte $20,000 par victime
    - http://www.securityvibes.com/community/fr/blog/2010/09/06/fraude-nig%C3%A9riane-20-000-de-gain-par-victime-en-moyenne
- Une conférence pour les "méchants"
    - http://malcon.org/
- Des malwares pour Nintendo DS / Wii ?
    - http://games.venturebeat.com/2010/07/31/live-demos-of-hacking-the-nintendo-ds-and-the-wii-to-spread-malware/

Actualité (francophone)

- http://france.fr/
  - L'échec ...
- ARJEL vs. StanJames
  - L'ARJEL obtient en justice le filtrage du site par les FAI français
    - Un précédent inquiétant
    - Même si le site a finalement décidé de bloquer de lui-même les clients français
- VAE "ESSI"
    - http://www.ssi.gouv.fr/site_rubrique130.html

Actualité (francophone)

- Les premiers emails "HADOPI" sont frauduleux
  - http://www.itespresso.fr/hadopi-a-peine-instauree-on-signale-deja-des-tentatives-de-fraudes-36446.html
- L'Etat, coupable de négligence caractérisée ?
  - http://bluetouff.com/2010/09/11/scandale-sites-gouvernementaux-negligence-caracterisee/
- Le ministère des affaires étrangères victime de typosquatting
  - https://pastel.diplomatie.gouv.fr/editorial/actual/ael2/pointpresse.asp?liste=20100715.html#Chapitre9

Actualité (anglo-saxonne)

- Conférences BlackHat/DefCon
  - Cf. compte-rendu de ce jour à l'OSSIR
  - Résultats du concours "Pwnie Award 2010"
    - http://pwnies.com/winners/
  - DefCon et le badge "Ninja"
    - De plus en plus élaboré
    - http://www.wired.com/threatlevel/2010/07/defcon-ninja-badge/
  - L'échec de la serrure biométrique
    - Il existe un *fallback* extrêmement simple à crocheter
    - http://www.wired.com/threatlevel/2010/07/lock-cracks/

Actualité (anglo-saxonne)

- Deviennent légaux aux USA …
  - La copie de DVD protégés par CSS
  - Le "jailbreaking" de téléphones
    - http://www.copyright.gov/1201/2010/Librarian-of-Congress-1201-Statement.html
- FireFox devient le navigateur officiel chez IBM
    - http://www.sutor.com/c/2010/07/ibm-moving-to-firefox-as-default-browser/
- Un cadre d'Apple arrêté pour espionnage industriel
    - http://online.wsj.com/article/SB10001424052748704023404575429730852274418.html?mod=WSJEUROPE_hpp_sections_tech
- Les USA vont-ils manquer de "cyberwarriors" ?
    - http://www.npr.org/templates/story/story.php?storyId=128574055
- Les USA vers une identité dans le "Cyberspace" ?
    - http://www.cs.columbia.edu/~smb/blog//2010-07/2010-07-11.html

Actualité (européenne)

- **IBM attaqué devant la commission européenne pour abus de position dominante**
  - **Sur le marché des *mainframes***

Actualité (Google)

- Google Instant Search
  - http://www.google.fr/instant/
- Google relance le débat sur le "full disclosure"
  - http://googleonlinesecurity.blogspot.com/2010/07/rebooting-responsible-disclosure-focus.html
- … ainsi que le débat sur la "neutralité du Net"
  - L'Internet mobile ne serait pas l'Internet
    - http://googlepublicpolicy.blogspot.com/2010/08/joint-policy-proposal-for-open-internet.html
- Un service "anti piratage" pour les applications Android
  - http://android-developers.blogspot.com/2010/07/licensing-service-for-android.html
  - Note: il est déjà piraté ☺
- Le premier *rootkit* pour Android présenté à BlackHat
  - Aucune révolution technologique: il s'agit d'un *rootkit* Linux classique
    - http://www.h-online.com/security/news/item/Android-rootkit-demonstrated-1049183.html

Actualité (Google)

- Il y aura un "Chrome Market"
  - La beta est disponible
    - http://blog.chromium.org/2010/08/get-your-apps-ready-for-chrome-web.html
- Google rachète Slide.com
  - Et prépare son propre réseau social ?
    - http://googleblog.blogspot.com/2010/08/google-and-slide-building-more-social.html
- Google rachète Like.com
  - Pour intégrer la technologie à Google Googles ?
- Mort annoncée de Google Wave
    - http://www.informationweek.com/news/software/open_source/showArticle.jhtml?articleID=226600016

Actualité (Google)

- Le problème de la gestion des failles "multi vendeurs"
  - Exemple: libPNG
    - http://code.google.com/p/chromium/issues/detail?id=45983#c17
- Google va-t-il devoir publier son algorithme d'indexation ?
  - Pour éviter une situation de concurrence déloyale ...
    - http://www.nytimes.com/2010/07/15/opinion/15thu3.html?_r=4
- Google Alarm
  - Pour mesurer l'étendue du problème …
    - http://fffff.at/google-alarm/
- … ou le plus officiel "Google Analytics Opt-Out"
    - http://tools.google.com/dlpage/gaoptout

Actualité (crypto)

- Une attaque sur AES ?
  - http://arxiv.org/abs/1006.5894

- La crypto quantique … encore cassée !
  - http://www.lefigaro.fr/sciences-technologies/2010/08/30/01030-20100830ARTFIG00635-reputee-inviolable-la-securite-quantique-a-ete-hackee.php

Actualité

- Conférences
  - Xcon 2010
    - http://twitter.com/dm557/status/20287749553
- Sorties
  - TrueCrypt 7.0
  - Backtrack 4 R1
    - 100% compatible VMWare
  - NoScript 2.0
    - Plus de support FireFox 2.x
  - VirtualBox 3.2.8
    - Correction de failles ?
  - VASTO (Virtualization Assessment Toolkit)
    - http://vasto.nibblesec.org/
  - Secunia PSI 2.0 (Beta)
    - http://secunia.com/blog/127/

Actualité

- Rapid7 "sponsorise" W3AF
  - Après Metasploit
    - http://blog.metasploit.com/2010/07/w3af-open-source-success-story.html
- HP rachète ArcSight (SIEM)
  - Pour un montant de $1,5 milliard

Actualité

- BlackBerry et iPhone vivement déconseillés en Allemagne
  - Pas assez sûrs ?
    - http://www.rtbf.be/info/economie/espionnage-les-ministres-allemands-pries-de-bannir-iphone-et-blackberry-243979
- Le BlackBerry (aurait pu être) interdit au Moyen Orient
  - Pas assez contrôlable ?
    - http://www.20minutes.fr/article/587051/High-Tech-Les-pays-du-Golfe-veulent-interdire-les-principaux-services-sur-BlackBerry.php
  - Les gouvernements concernés ont obtenu gain de cause
- L'EFF demande à Verizon de révoquer le certificat racine Etisalat
  - Une menace pour la sécurité du SSL ?
    - https://www.eff.org/deeplinks/2010/08/open-letter-verizon

Actualité

- Oracle attaque Google pour violation de brevet sur la technologie Java
  - Une mauvaise nouvelle pour les développeurs Java ?
    - http://java.dzone.com/articles/oracle-sues-google-over
- Les failles logicielles affectent gravement les équipements médicaux implantables
  - 6 équipements sur 23 retirés de la vente depuis début 2010 pour une raison logicielle
    - http://www.softwarefreedom.org/resources/2010/transparent-medical-devices.html
- Un chercheur arrêté en Inde
  - Il avait démontré des failles dans les machines à voter
  - Et refusé d'expliquer qui lui a procuré le matériel
    - http://www.wired.com/threatlevel/2010/08/researcher-arrested-in-india
- Dell a (sciemment) vendu 12 million de cartes mères défectueuses
    - http://www.lemonde.fr/technologies/article/2010/06/30/dell-a-vendu-12-millions-d-ordinateurs-defectueux_1380926_651865.html

Fun

- La protection HDCP cassée
  - La "clé maitre" est disponible
    - http://www.engadget.com/2010/09/14/hdcp-master-key-supposedly-released-unlocks-hdtv-copy-protect/
    - http://pastebin.com/kqD56TmU
- La PS3 "jailbreakée"
  - Par un *dongle* USB destiné au débogage de la console
    - http://www.planetadejuego.com/tutorial-psjailbreak-modchip

Fun

- Le service de sécurité du président russe piraté
  - Le mot de passe par défaut n'avait pas été changé
    - http://tempsreel.nouvelobs.com/actualite/monde/20100824.OBS8917/russie-des-hackers-piratent-le-service-de-protection-de-poutine-et-medvedev.html
- Un site Symantec piraté
  - Le site http://www.hackiswack.com/
  - … destiné à lutter contre le "cybercrime"
    - http://www.theregister.co.uk/2010/09/03/symantec_rap_contest_farce/
- Un "trolleur" démasqué grâce à un lien "TinyURL"
  - Sur la liste OpenBSD
    - http://www.mail-archive.com/misc@openbsd.org/msg94265.html
- Un *fuzzer* … pour lecteurs de code-barre
    - http://www.irongeek.com/i.php?page=security%2Fbarcode-flashing-led-fuzzer-bruteforcer-injector

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 12 octobre 2010
- N'hésitez pas à proposer des sujets et des salles