OSSIR
Groupe Paris

Réunion du 10 novembre 2009

Revue des dernières vulnérabilités

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

Avis Microsoft (1/15)

- **Correctif d'Octobre 2009**
  - **Avec [exploitability index]**
    - **13 bulletins (34 failles) = plus gros score Microsoft**
      - **http://blogs.technet.com/srd/archive/2009/10/12/assessing-the-risk-of-the-october-security-bulletins.aspx**

Deployment Priority

Based on a combination of severity rating, exploitability index rating, available mitigations and workarounds and range of affected products. All customers should perform their own prioritization assessment as each environment is different and other factors may apply. Microsoft recommends that all security updates be deployed as soon as possible. This priority slide is provided "AS IS" with no warranties, and confers no rights.

Bulletin	KB	Public	Aggregate Severity	Exploit Index	Max Impact	Deployment Priority	Note
WMR MS09-051	975682	Yes	Critical	1	RCE	1	Browse and own through all supported OS's (except Win7 and Server 2008 R2). Easy to achieve reliable exploit. Limited attacks in the wild. Main Target: End user systems
SMB MS09-050	975517	Yes	Critical	1	RCE	1	Unauthenticated remote code execution. SMB typically blocked by edge firewalls so attacks more likely from local subnet. Main Target: Servers and Workstations
IE MS09-054	974455	Yes	Critical	1	RCE	1	Browse and own through all supported OS's. Easy to achieve reliable exploit. One vuln disclosed publicly. Main Target: End user systems
.NET CLR MS09-061	974378	Yes	Critical	1	RCE	1	Browse and own through all supported OS's with .NET Framework 1.1. PoC code publicly disclosed. Main Target: End user systems
GDI+ MS09-062	957488	No	Critical	1	RCE	1	Browse and own scenario Main Target: End user systems
WMP MS09-032	974112	No	Critical	1	RCE	1	Browse and own through Win2000, XP and Server 2003. Main Target: End user systems
Indexing Service MS09-057	960859	No	Important	2	RCE	2	Indexing Service not installed by default. Main Target: Servers and Workstations
ActiveX Kill Bit MS09-055	973525	No	Critical	2	RCE	2	Kill bits for ATL controls. Responsibly disclosed, no known attacks. Main Target: End user systems
Office ATL MS09-060	973885	No	Critical	2	RCE	2	Binary updates for ATL controls. Responsibly disclosed, no known attacks. Main Target: End user systems
IIS MS09-053	975254	Yes	Important	2	RCE	2	FTP service not installed by default. RCE possible only on Win2008. Main Target: Servers
LSASS MS09-059	975467	Yes	Important	3	DoS	3	Denial of Service only. Main Target: Servers and Workstations
Kernel MS09-058	971486	No	Important	3	EoP	3	Local logon required. Elevation of Privilege only. Main Target: Terminal Servers and Workstations
CryptoAPI MS09-056	974571	Yes	Important	3	Spoof	3	Spoofing attack only, no code execution. Main Target: End user systems

Avis Microsoft (2/15)

- MS09-050 Failles SMBv2 [3,1,1]
  - Affecte: Windows Vista et 2008
  - Exploit:
    - Déni de service (x1)
    - Exécution de code (x2)
      - ... à distance, en mode noyau, sans authentification, via un paquet SMBv2 malformé
  - Crédit: Matthieu Suiche
  - Note:
    - http://blogs.technet.com/srd/archive/2009/10/12/ms09-050-threat-landscape-for-the-smb-bulletin.aspx
    - http://blogs.msdn.com/sdl/archive/2009/10/15/ms09-050-smbv2-and-the-sdl.aspx

Avis Microsoft (3/15)

- MS09-051 Failles dans Windows Media Runtime [1,2]
  - Affecte: Windows (toutes versions supportées sauf Seven et 2008 R2)
  - Exploit:
    - Exécution de code à l'ouverture d'un fichier ASF malformé
    - Exécution de code à l'ouverture d'un fichier malformé
  - Crédit:
    - Ivan Fratric / ZDI
    - Jun Xie / McAfee
    - Vinay Anantharaman / Adobe
  - Note:
    - http://blogs.technet.com/srd/archive/2009/10/12/ms09-051-a-note-on-the-affected-platforms.aspx

- MS09-052 Faille dans Windows Media Player [1]
  - Affecte: Windows Media Player 6.4
  - Exploit: exécution de code à l'ouverture d'un fichier ASF malformé
  - Crédit: Yamata Li / Palo Alto Networks

Avis Microsoft (4/15)

- MS09-053 Failles dans le serveur FTP [3,1]
  - Affecte: FTP (toutes versions supportées sauf IIS 7.5)
  - Exploit:
    - Déni de service
    - Exécution de code
  - Crédit: Kingcope (x2)

Avis Microsoft (5/15)

- MS09-054 Patch cumulatif pour IE [2,1,2,2]
  - Affecte: IE (toutes versions supportées)
    - Ainsi que FireFox si le .NET Framework est installé (!)
  - Exploit:
    - http://skypher.com/index.php/2009/10/13/ms09-054cve-2009-1547-data-stream-header-corruption-vulnerability/
  - Crédit:
    - SkyLined / Google
    - ZDI
    - Sam Thomas / ZDI
  - Note:
    - http://blogs.technet.com/srd/archive/2009/10/12/ms09-054.aspx
    - La fondation Mozilla ajoute le plugin WPF dans sa liste noire
      - http://blog.mozilla.com/security/2009/10/16/net-framework-assistant-blocked-to-disarm-security-vulnerability/
      - https://www.mozilla.com/en-US/blocklist/

Avis Microsoft (6/15)

- MS09-055 Mise à jour des KillBits [n/a]
  - Affecte:
    - Windows Live Mail Components
    - Office Web Components
    - Outlook View Controls
    - Visio Viewer
    - MSN Photo Upload Tool
  - Exploit: contrôles compilés avec une version ATL vulnérable
  - Crédit: n/d

- MS09-056 Failles dans la CryptoAPI [3,3]
  - Affecte: Windows (toutes versions supportées)
  - Exploit:
    - Mauvais traitement des certificats contenant un caractère NULL
    - Integer Overflow dans le parser ASN1
  - Crédit:
    - Ian Wright & Jean-Luc Giraud / Citrix
    - Dan Kaminsky / IOActive
  - Note:
    - http://blogs.technet.com/srd/archive/2009/10/12/ms09-056-addressing-the-x-509-cryptoapi-asn-1-security-vulnerabilities.aspx

Avis Microsoft (7/15)

- **MS09-057 Faille dans le service d'indexation [2]**
  - **Affecte: Windows 2000 / XP / 2003**
  - **Exploit: contrôle ActiveX vulnérable**
  - **Crédit: Yamata Li / Palo Alto Networks**

- **MS09-058 Failles noyau [2,3,3]**
  - **Affecte: Windows (toutes versions supportées sauf Seven et 2008 R2)**
  - **Exploit:**
    - ***Integer Underflow***
    - **Déréférencement de pointeur NULL**
    - **Déni de service lié à un gestionnaire d'exception**
  - **Crédit:**
    - **Tavis Ormandy & Neel Mehta / Google**
    - **NSFocus Security Team**
    - **Tavis Ormandy & Neel Mehta / Google**

Avis Microsoft (8/15)

- **MS09-059 Faille dans LSASS [3]**
  - **Affecte: Windows (toutes versions supportées sauf Windows 2000)**
  - **Exploit: *Integer Overflow***
  - **Crédit: n/d**

- **MS09-060 Failles ATL dans les contrôles ActiveX Office (x3) [2]**
  - **Affecte: Office (toutes versions supportées) + Visio**
  - **Exploit: exécution de code via des contrôles ActiveX installés par Office**
  - **Crédit:**
    - **David Dewey / IBM ISS X-Force**
    - **Ryan Smith / iDefense Labs (x2)**

Avis Microsoft (9/15)

- MS09-061 Failles dans le Framework .NET [1,1,1]
  - Affecte: .NET Framework 1.0 / 1.1 / 2.0 + SilverLight 2
  - Exploit:
    - Exécution de code possible par tout composant .NET (SilverLight, ASP.NET, XBAP, ...)
      - Récupération d'un pointeur dans du code managé
      - Transtypage incorrect d'objets
      - Accès mémoire en dehors du Framework
  - Crédit:
    - Pavel Minaev
    - Jeroen Frijters / Sumatra
  - Note:
    - http://blogs.technet.com/srd/archive/2009/10/12/ms09-061-more-information-on-the-net-security-bulletin.aspx

Avis Microsoft (10/15)

- **MS09-062 Failles GDI+ [2,2,2,1,2,2,1,2]**
  - **Affecte: GDI+**
    - **Windows / IE / .NET / Office / SQL Server / Visual Studio / ForeFront Client**
  - **Exploit:**
    - **Fichier WMF malformé (Integer Overflow)**
    - **PNG (Heap Overflow)**
    - **TIFF (Buffer Overflow)**
    - **TIFF (corruption mémoire)**
    - **Evasion de la VM .NET (Integer Overflow dans RSClientPrint)**
    - **PNG (Integer Overflow)**
    - **Corruption mémoire à l'ouverture d'un dessin Office**
    - **Office BMP (Integer Overflow)**
  - **Crédit:**
    - **Yamata Li / Palo Alto Networks**
    - **Thomas Garnier / SkyRecon**
    - **Wushi / iDefense Labs**
    - **Ivan Fratric / ZDI ; Tavis Ormandy of Google Inc. ; Carlo Di Dato (aka shinnai)**
    - **Tavis Ormandy / Google Inc.**
    - **Marsu Pilami / iDefense Labs**
    - **Carsten H. Eiram / Secunia**

Avis Microsoft (11/15)

- Compléments
  - La faille TIFF a été "vendue" en décembre 2007
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=828
  - La faille "Office" a été "vendue" en avril 2008
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=829

Avis Microsoft (12/15)

- A noter également
  - MS09-062 ajoute la sélection de formats supportés par GDI+
    - Anciennement disponible dans un patch optionnel
      - http://support.microsoft.com/KB/958911
- Prévisions pour Novembre 2009
  - 6 bulletins
    - 3 critiques, 3 important
    - corrigeant 15 failles

Avis Microsoft (13/15)

- Advisories
  - 973811 est complété par MS09-054
    - "*Extended Protection for Authentication*"
      - Permet de contrôler le SSO Windows (*credential forwarding*)
  - 973882 est complété par MS09-060 (ATL)
  - 975191 devient MS09-053 (FTP)
  - 975497 devient MS09-050 (SMBv2)

Avis Microsoft (14/15)

- Révisions
  - MS08-069
    - V3.0: le composant vulnérable est parfois installé par des applications tierces sur Windows 2008 R2 et Seven
  - MS09-024
    - V1.1: support des versions localisées de Works 9
  - MS09-043
    - V2.0: problème d'installation du correctif avec Office 2003 SP3
  - MS09-044
    - V2.1: nouveau problème connu
  - MS09-046
    - V1.1: correction du CLSID
  - MS09-050
    - V1.1: mise à jour de la FAQ
  - MS09-051
    - V1.1: correction du CVE (attaques détectées dans la nature)
  - MS09-052
    - V1.1: solution de contournement inefficace

Avis Microsoft (15/15)

- MS09-053
  - V1.1: suppression des crédits (!), IIS 6.0 présent sur XP64 SP2
- MS09-054
  - V1.1: informations complémentaires pour les utilisateurs de FireFox
  - V1.2: ajout d'un problème connu
  - V2.0: problèmes de compatibilité détectés, nouveau correctif
- MS09-055
  - V1.1: correction du lien pour Windows XP64 SP2, correction du CVE
  - V1.2: mise à jour de la FAQ (particulièrement sur Visio Viewer 2007)
- MS09-059
  - V1.1: correction du CVE
- MS09-060
  - V1.1: documentation de problèmes connus
  - V1.2: Visio Viewer 2007 n'est pas affecté
- MS09-061
  - V1.1: corrections documentaires
  - V1.2: mise à jour de la FAQ
- MS09-062
  - V1.1: SQL Server Express SP3 n'est pas affecté
  - V2.0: Visio Viewer 2007 est affecté, SQL Server 2008 n'est pas affecté
  - V2.1: Visio Viewer 2007 n'est pas affecté

Infos Microsoft

- **Sorties logicielles**
  - **Windows Seven et Windows 2008 R2**
  - **Visual Studio 2010 / .NET Framework 4.0 (Beta 2)**
  - **Microsoft Baseline Security Analyzer 2.1.1**
    - **Supporte Windows Seven et 2008 R2**
  - **Microsoft Web Protection Library (en préparation)**
    - **http://blogs.msdn.com/securitytools/archive/2009/10/17/web-protection-library-ctp-release-coming-soon.aspx**
  - **Enhanced Mitigation Evaluation Toolkit (EMET)**
    - **http://go.microsoft.com/fwlink/?LinkID=162309**
    - **Permet d'ajouter sans recompilation les options suivantes:**
      - **SEHOP**
      - **DEP**
      - **User-mode NULL pointers**
      - **Heap Spray**

Infos Microsoft

- **Autre**
  - **Microsoft Security Intelligence Report, volume 7**
    - **http://www.microsoft.com/sir**
  - **L'Exploitability Index serait peu fiable**
    - **http://news.techworld.com/security/3205509/microsofts-calls-on-bug-exploits-worse-than-coin-toss**
  - **Gartner encourage les entreprises à passer rapidement sous Seven**
    - **http://www.lemagit.fr/article/gartner-migration-windows-7-windows-vista/4534/1/gartner-encourage-les-entreprises-migrer-rapidement-sous-windows-7/**
  - **Des infos sur Windows 8**
    - **Un cas d'école de collecte d'informations sur Internet !**
      - **http://www.techradar.com/news/software/operating-systems/8-things-you-need-to-know-about-windows-8-643699**
  - **Communication Microsoft ... FAIL ?**
    - **http://technet.microsoft.com/fr-fr/ee663025.aspx**

Infos Réseau

- **Principales failles**
  - **SSLv3 / TLSv1 vulnérable à un "man in the middle"**
    - **Durant la phase de renégociation des clés**
      - **http://isc.sans.org/diary.html?storyid=7534**
      - **http://seclists.org/fulldisclosure/2009/Nov/62**
  - **TKIP à nouveau attaqué**
    - **D'un paquet ARP ... à un paquet DHCP**
      - **http://books.google.com/books?id=mSMsqoqufMoC&pg=PA120&source=gbs_toc_r&cad=4#v=onepage&q=&f=false**

Infos Réseau

- **Autres infos**
  - **Le nouveau propriétaire de "blackhole.us" en a marre ...**
    - **... et met en place un wildcard DNS**
      - **http://seclists.org/nanog/2009/Oct/458**
  - **Le TLD ".se" disparait d'Internet pendant quelques heures**
    - **http://www.presence-pc.com/actualite/TLD-Suede-Internet-36775/**
  - **Le RIPE accusé de travailler pour RBN**
    - **http://www.eweekeurope.co.uk/news/russian-police-and-internet-registry-accused-of-aiding-cybercrime-2165**
    - **Réponse du RIPE**
      - **http://www.ripe.net/news/rbn.html**

Infos Réseau

- Les TLD s'internationalisent
  - http://www.lefigaro.fr/web/2009/10/30/01022-20091030ARTFIG00562-les-adresses-web-s-ecriront-dans-tous-les-alphabets-.php
- Cisco rachète ScanSafe
- Communication Cisco
  - http://www.cisco.com/cdc_content_elements/flash/security/therealm/index.html

Infos Unix

- (Principales) failles
  - Faille dans PHPMyAdmin
    - Affecte: PHPMyAdmin 2.x et 3.x
    - Exploit: injection SQL dans l'interface de génération PDF
      - http://www.phpmyadmin.net/home_page/security/PMASA-2009-6.php
  - Faille dans ZFS
    - Affecte: Solaris 10
    - Exploit: vol de fichiers via ZFS
      - http://sunsolve.sun.com/search/document.do?assetkey=1-66-265908-1
  - Failles multiples dans xpdf et dérivés
    - Affecte: xpdf, gpdf, kpdf, cups, etc.
    - Exploit: exécution de code à l'ouverture d'un fichier malformé
      - http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-448/CERTA-2009-AVI-448.html

Infos Unix

- Déréférencement de pointeur NULL dans "fs/pipe.c"
  - Affecte: au moins Linux 2.6.21 -> 2.6.31
    - http://lkml.org/lkml/2009/10/14/184
- Faille dans GD
  - Affectant PHP < 5.2.11 et corrigée silencieusement
    - http://www.openwall.com/lists/oss-security/2009/10/15/13
- Nombreuses failles dans des modules tiers pour Drupal
    - http://drupal.org/forum/44

Infos Unix

- **Failles BSD**
  - **Déni de service distant dans le serveur SMTP d'OpenBSD**
    - **Trivial ... et non catégorisé comme faille de sécurité**
      - **http://xorl.wordpress.com/2009/10/14/openbsd-smtpd-remote-crash/**
  - **OpenBSD supporte (à peine) le MMX**
    - **http://xorl.wordpress.com/2009/10/16/openbsd-i386-xmm-unhandled-exception/**
  - **Failles dans printf()**
    - **Affecte: OpenBSD 4.6, NetBSD 5.0.1**
    - **Exploit: printf %*********s 666**
      - **http://securityreason.com/achievement_securityalert/69**

Infos Unix

- **Autre**
  - **Sortie d'OpenBSD 4.6**
    - **http://marc.info/?l=openbsd-misc&m=125588091023791&w=2**
    - **http://www.openbsd.org/errata46.html**
  - **Debian met en place un suivi des failles de sécurité**
    - **http://security-tracker.debian.org/tracker/**
  - **GCC va supporter le "link-time optimization"**
    - **http://nickclifton.livejournal.com/4128.html**

Failles

- **Principales applications**
  - **Adobe Acrobat < 8.1.7, < 9.2.0**
    - **(et toutes les versions antérieures)**
    - **Pas moins de 29 failles corrigées par le patch du 13 octobre**
  - **Quaterly patch d'Oracle**
    - **38 failles corrigées**
      - **... dont 16 affectant directement la base de données, parmi lesquelles 6 exploitables à distance**
    - **http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html**
  - **Failles multiples dans VMWare**
    - **En particulier le client ISC DHCP**
      - **http://lists.vmware.com/pipermail/security-announce/2009/000067.html**
    - ***Directory Traversal*, élévation de privilèges dans l'invité**
      - **http://lists.vmware.com/pipermail/security-announce/2009/000069.html**
      - **Crédit: Tavis Ormandy & Julien Tinnès**

Failles

- FireFox < 3.0.15, 3.5.4
  - http://www.mozilla.org/security/known-vulnerabilities/firefox35.html#firefox3.5.4
- FireFox 3.5.5 ne corrige pas de failles de sécurité (a priori)
- Chrome < 3.0.195.32
  - http://googlechromereleases.blogspot.com/2009/11/stable-channel-update.html
- Opera < 10.01
  - http://www.opera.com/support/kb/view/938/
  - http://www.opera.com/support/kb/view/939/
  - http://www.opera.com/support/kb/view/940/
- WireShark < 1.2.3
  - http://www.wireshark.org/security/wnpa-sec-2009-07.html
  - http://www.wireshark.org/security/wnpa-sec-2009-08.html

Failles

- ShockWave < 11.5.2.602
  - 4 failles trouvées par Nicolas Joly / VUPEN
    - http://www.adobe.com/support/security/bulletins/apsb09-16.html
- Java 1.6.0_16
  - Pas de faille de sécurité corrigée a priori
    - http://java.sun.com/javase/6/webnotes/6u16.html
- Java 1.6.0_17
  - Plusieurs failles de sécurité corrigées (cf. bulletins ZDI et iDefense)
    - http://java.sun.com/javase/6/webnotes/6u17.html
- BlackBerry Desktop Software < 5.01
    - http://www.blackberry.com/btsc/viewContent.do?externalId=KB19701

Failles

- La faille de Joanna R. sur les BIOS Q35/Q45 corrigée
  - http://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00020&languageid=en-fr

Failles 2.0

- Encore une initiative de sécurité déclarative pour lutter contre XSS et XSRF
  - Mozilla Content Security Policy
    - https://wiki.mozilla.org/Security/CSP
  - (Du même acabit que la protection contre le Click-Jacking)
    - http://blogs.msdn.com/ie/archive/2009/01/27/ie8-security-part-vii-clickjacking-defenses.aspx
- L'auteur de Stoned Bootkit travaille pour un gang de malwares
  - Ou bien est-ce juste un ado en mal de reconnaissance ?
    - http://cert.lexsi.com/weblog/index.php/2009/10/22/344-jeux-de-dupe
- Des éditeurs d'applications Facebook piratés
    - http://thompson.blog.avg.com/2009/10/hacked-facebook-applications-reach-out-to-exploit-sites-in-russia.html

Malwares et spam

- **URLZone / Bebloh, le malware bancaire du futur**
  - **Attend la saisie de tous les codes**
    - **En cas d'authentification 2 facteurs**
  - **Vérifie l'état du compte avant tout transfert**
  - **Transfert une fraction du compte uniquement**
  - **Utilise des mules "innocentes" si exécuté dans une VM**

    - **http://bl0g.cedricpernet.net/post/2009/10/06/Les-surprises-d-URLZone**

Malwares et spam

- Facebook obtient $711m de dommages et intérêts suite à du spam
  - $50 par infraction
    - http://www.clubic.com/actualite-308618-spam-facebook-obtient-700-dommages.html
- Les iPhones hollandais "jailbreakés" victimes de racket
  - En cause: le SSH ouvert avec un login/mot de passe connu
    - http://arstechnica.com/apple/news/2009/11/dutch-hacker-holds-jailbroken-iphones-hostage-for-5.ars
- Peu de temps après, un ver se propage sur les iPhones australiens
  - Même mécanisme
    - http://isc.sans.org/diary.html?storyid=7549
- Les membres du groupe "m00p" poursuivis en justice
  - Pour des faits remontant à 2005 ...
    - http://www.f-secure.com/weblog/archives/00001804.html
- Kaspersky lance un antivirus pour Mac OS X

Actualité (France)

- La mairie de NKM victime d'attaques informatiques
  - http://www.zdnet.fr/actualites/internet/0,39020774,39710262,00.htm
  - C'est probablement la faute aux antivirus ☺
    - http://twitter.com/nk_m/status/5563664369
- Une messagerie sécurisée pour les médecins en 2010 ?
  - http://www.conseil-national.medecin.fr/index.php?url=presse/article.php&id=165
- Création de "l'institut national des hautes études de la sécurité et de la justice"
  - http://www.net-iris.fr/veille-juridique/actualite/23303/creation-de-institut-national-des-hautes-etudes-de-la-securite-et-de-la-justice.php
- Le RSSI à temps partagé
  - http://www.plenium.fr/offre/responsable_informatique_temps_partage_pme.php
- La carte TOOAL certifiée CSPN
  - http://www.ssi.gouv.fr/site_article136.html

Actualité (anglo-saxonne)

- Apps.gov: le portail "cloud" du gouvernement américain
  - https://apps.gov/cloud/advantage/main/start_page.do
  - http://www.whitehouse.gov/blog/Streaming-at-100-In-the-Cloud/
- La DARPA lance un projet de recherche pour créer un nouveau réseau militaire
  - MNP: Military Network Protocol
- Les anglais lancent la Hacker Academy
  - Toujours le même problème: recruter
    - http://www.lemonde.fr/technologies/article/2009/10/14/la-grande-bretagne-lance-sa-hacker-academy_1253678_651865.html
- MobileSpy pour BlackBerry: $100
  - http://www.mobile-spy.com/spy-blackberry.html

Actualité (anglo-saxonne)

- Les internautes américains ont conscience des risques
  - Mais ne font rien pour s'en protéger
    - http://www.staysafeonline.org/content/2009-cyber-security-study
- La CIA sous-traite la surveillance des réseaux sociaux
    - http://www.visibletechnologies.com/
- La NSA estime devoir stocker 1 YottaOctet de données en 2015
    - http://www.nybooks.com/articles/23231
- Le premier centre de Cyber Sécurité ouvert aux Etats-Unis
    - http://www.lemonde.fr/technologies/article/2009/11/02/inauguration-aux-etats-unis-du-premier-centre-unifie-de-cyber-securite_1261535_651865.html
- Une panne informatique provoque un dysfonctionnement des feux de circulation
  - A Washington DC, pendant plusieurs jours
    - http://www.wtop.com/?sid=1803146

Actualité (anglo-saxonne)

- Négociations "Anti-Counterfeiting Trade Agreement" (ACTA)
  - Le grand filtrage se prépare
    - http://www.michaelgeist.ca/content/view/4510/125/
- Injection SQL sur le site BarackObama.com
  - Notez que l'auteur s'était déjà attaqué à la BNP et au Crédit Agricole
    - http://unu1234567.baywords.com/2009/10/26/barackobama-com-full-acces-sql-injection/
  - Les détails techniques
    - http://praetorianprefect.com/archives/2009/10/the-barack-obama-donations-site-was-hacked%E2%80%A6err-no-it-wasn%E2%80%99t/

Actualité (crypto)

- Attaque DPA à distance sur téléphones portables
  - http://news.cnet.com/8301-27080_3-10379115-245.html

Actualité

- Rapid7 "achète" Metasploit
  - http://www.rapid7.com/metasploit-announcement.jsp
  - http://blog.metasploit.com/2009/10/metasploit-rising.html
- Ca bouge dans la sécurité Web
  - M86 achète Finjan
  - Barracuda Networks achète PureWire
- Skype bientôt disponible en Open Source ?
  - http://ofaurax.free.fr/blog/index.php5/2009-10-31-00h31-0100.xml

Actualité

- L'attaque la femme de ménage vs. TrueCrypt
  - http://theinvisiblethings.blogspot.com/2009/10/evil-maid-goes-after-truecrypt.html
  - Remarque: c'est une attaque crédible ...
    - http://www.wired.com/threatlevel/2009/11/mossad-hack/
- TrueCrypt 6.3 disponible
  - Support de Windows Seven et Mac OS X 10.6
- Produits VMWare
  - Workstation 7.0
  - Fusion 3.0
  - ACE 2.6
- WordPress 2.8.5 "hardening release"
  - http://wordpress.org/development/2009/10/wordpress-2-8-5-hardening-release/

Actualité

- "Closed Source" défini comme "Nearly Open Source" par le parlement européen
  - http://www.computerworlduk.com/community/blogs/index.cfm?entryid=2620&blogid=14
- Le "paquet télécom" impose aux FAI de communiquer sur leurs pertes de données
  - http://www.out-law.com/page-10497
- Discussion autour des données SWIFT
  - Un vieux serpent de mer
    - http://www.senat.fr/leg/ppr09-072.html
- Le filtrage d'Internet ne servirait à rien
  - http://cybercriminalite.wordpress.com/2009/10/27/europe-une-etude-detruit-encore-lefficacite-du-filtrage-dinternet/
- La Suède autorise l'écoute de toute conversation en transit sur le sol Suédois
  - Résultat: le site des services secrets "www.fra.se" est victime d'un DDoS
    - http://www.f-secure.com/weblog/archives/00001808.html

Actualité

- L'ISO 27001 rend-t-elle plus sûr ?
  - http://www.zdnet.fr/blogs/securite-it/utile-l-iso-27001-mouais-39709736.htm
- Le logiciel qui détecte les attaques
  - ... et se corrige lui-même
    - http://www.technologyreview.com/computing/23821/
- Des militaires déployés autour des sites High-Tech indiens
  - http://pro.01net.com/editorial/506859/des-commandos-pour-assurer-la-securite-des-ssii/
- Analyse d'une machine à voter
  - http://studysequoia.wikispaces.com/
- Publication de la norme "WiFi Direct"
  - http://www.wi-fi.org/news_articles.php?f=media_news&news_id=909

Actualité

- Les détails de l'intrusion chez Wal-Mart (2006)
  - http://www.wired.com/threatlevel/2009/10/walmart-hack/
- Le Département fédéral des affaires étrangères (Suisse) victime d'une attaque très ciblées
  - http://www.news.admin.ch/dokumentation/00002/00015/index.html?lang=fr&msg-id=29701

Fun

- Un émulateur NES en JavaScript
  - http://benfirshman.com/projects/jsnes/
- Yahoo! en fait trop pour ses clients
  - http://www.brisbanetimes.com.au/technology/technology-news/yahoo-apologises-for-lap-dance-at-hack-event-20091021-h7sr.html
- Un hacker fait chanter Belgacom
  - *Download or die*
    - http://www.rtbf.be/info/societe/internet/un-hacker-veut-faire-chanter-belgacom-152625
- "Certifications are Evil"
  - http://cfed-ttf.blogspot.com/2009/10/certifications-are-evilby-john-mccash.html

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 8 décembre 2009
- N'hésitez pas à proposer des sujets et des salles