OSSIR
Groupe Paris

Réunion du 9 décembre 2008

Revue des dernières vulnérabilités

EdelWeb

Olivier REVENU
olivier.revenu (à) edelweb.fr

Mickaël DEWAELE
mickael.dewaele (à) edelweb.fr

Jérémy LEBOURDAIS
jeremy.lebourdais (à) edelweb.fr

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

Avis Microsoft (1/5)

- **Correctifs de Novembre 2008**

  - **MS08-068 Elévation de privilèges par "réflection" des authentifiants NTLM**
    - **Affecte: Windows (toutes versions supportées)**
    - **Exploit: permet la récupération d'authentifiants précédents**
    - **Crédit: n/d**
    - **Notes:**
      - **La signature SMB est un *workaround* efficace**
        - **http://blogs.technet.com/msrc/archive/2008/11/11/ms08-068-and-smbrelay.aspx**
        - **http://blogs.technet.com/swi/archive/2008/11/11/smb-credential-reflection.aspx**
        - **http://blog.metasploit.com/2008/11/ms08-067-metasploit-and-smb-relay.html**
      - **La faille aurait été trouvée en ... 1996 !**
        - **http://sid.rstack.org/blog/index.php/306-a-tout-seigneur-tout-honneur**

Avis Microsoft (2/5)

- **MS08-069 Vulnérabilités multiples dans le support XML (x3)**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit:**
    - **Exécution de code via un fichier XML malformé**
    - ***Cross-domain scripting* via une DTD spécifique**
    - **Fuite d'information *cross-domain* via un entête "transfer-encoding" spécifique**
  - **Crédit:**
    - **Gregory Fleischer**
    - **Stefano Di Paola / Minded Security**
    - **Robert Hansen / SecTheory**

Avis Microsoft (3/5)

- 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

- Advisories
  - Q956391
    - Mise à jour des "kill bits" pour 3 contrôles tiers
  - Q953839
    - FAQ: pourquoi Windows 2008 "core" se voit proposé les "kill bits"

Avis Microsoft (4/5)

- **Prévisions pour Décembre 2008**
  - **Bulletins critiques, "exécution de code à distance"**
    - **#1 Windows, toutes versions supportées**
    - **#2 Windows Vista et 2008**
    - **#3 Internet Explorer, toutes versions supportées**
    - **#4 Visual Basic et/ou VBA (?)**
      - **Versions spécifiques: Project, FoxPro, ...**
    - **#5 Word, toutes versions supportées**
    - **#6 Excel, toutes versions supportées**
  - **Bulletins importants**
    - **#7 SharePoint 2007, Search 2008**
      - **Elévation de privilèges**
    - **#8 Windows Media Center**
      - **"Exécution de code à distance"**

Avis Microsoft (5/5)

- Révisions
  - MS06-078
    - Version 6.1 : typo dans le nom de fichier
  - MS07-005
    - Version 2.0 : Windows XP SP3 est affecté
  - MS07-068
    - Version 2.3 : typo dans le nom de fichier
  - MS08-052
    - Version 2.2 : mise à jour de la FAQ, Visio Viewer n'est pas affecté
  - MS08-056
    - Version 1.1 : ce correctif ne peut pas être désinstallé
  - MS08-057
    - Version 1.2 : mise à jour de la FAQ
  - MS08-058
    - Version 1.2 : correction d'une clé de base de registre sur IE 6 / Windows 2003 64 bits
  - MS08-059
    - Version 1.2 : mise à jour des impacts pour le *workaround*
  - MS08-062
    - Version 2.2 : mise à jour de la FAQ
  - MS08-068
    - Version 1.1 : mise à jour de la FAQ

Infos Microsoft (1/9)

- Sorties logicielles
  - Microsoft Sync Framework 1.0
  - SilverLight 2
  - WinDbg 6.10.3.233

  - En "beta"
    - Vista SP2
    - OCS 2007 R2
    - Windows 2008 R2
    - .NET Framework 4.0
    - Windows Live Mesh
      - https://www.mesh.com/Welcome/Default.aspx
    - Windows Server "Dublin"
    - ILM "2"
    - Microsoft "Geneva" (pour la gestion d'identité)
      - https://connect.microsoft.com/site/sitehome.aspx?SiteID=642

Infos Microsoft (2/9)

- **Actualité**
  - **Microsoft travaille sur un concurrent de l'AppStore**
    - **http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9119552**
  - **Des outils pour protéger les applications Web**
    - **http://blogs.msdn.com/cisg/archive/2008/11/13/an-update-on-some-upcoming-free-tools.aspx**
    - **Anti-XSS 3.0**
    - **CAT.NET (audit de code intégré à Visual Studio)**

Infos Microsoft (3/9)

- Annonces autour du SDL
  - http://www.microsoft.com/sdl
  - SDL Optimization Model
  - SDL Pro Network
  - SDL Threat Modeling Tool (version 3.1 beta)
  - Kevlarr & The SDL
    - http://www.microsoft.com/security/bakingsecurityin/strips.htm

- *"MS08-014 – Security vulnerability could have been prevented by /W4 compilation"*
  - Source: Microsoft, WinHEC 2008

- Office 2007, "50% plus sûr" ?
  - http://blogs.msdn.com/david_leblanc/archive/2008/11/17/improvements-in-office-security.aspx

Infos Microsoft (4/9)

- Office 2007 SP2 permettra d'utiliser du chiffrement personnalisé
  - http://blogs.msdn.com/david_leblanc/archive/2008/12/04/new-improved-office-crypto.aspx
- One Care gratuit l'année prochaine : Microsoft "Morro"
  - http://www.microsoft.com/Presspass/press/2008/nov08/11-18NoCostSecurityPR.mspx
- Les outils pour webmaster de Microsoft vont aussi[*] détecter les malwares
  - [*] Google a annoncé la même chose il y a quelques semaines
  - http://blogs.msdn.com/livesearch/archive/2008/11/25/webmaster-tools-now-sniffing-for-malware.aspx
- Un nouveau site pour lutter contre les fraudes de type "loterie"
  - http://www.microsoft.com/france/securite/lottery/default.mspx

Infos Microsoft (5/9)

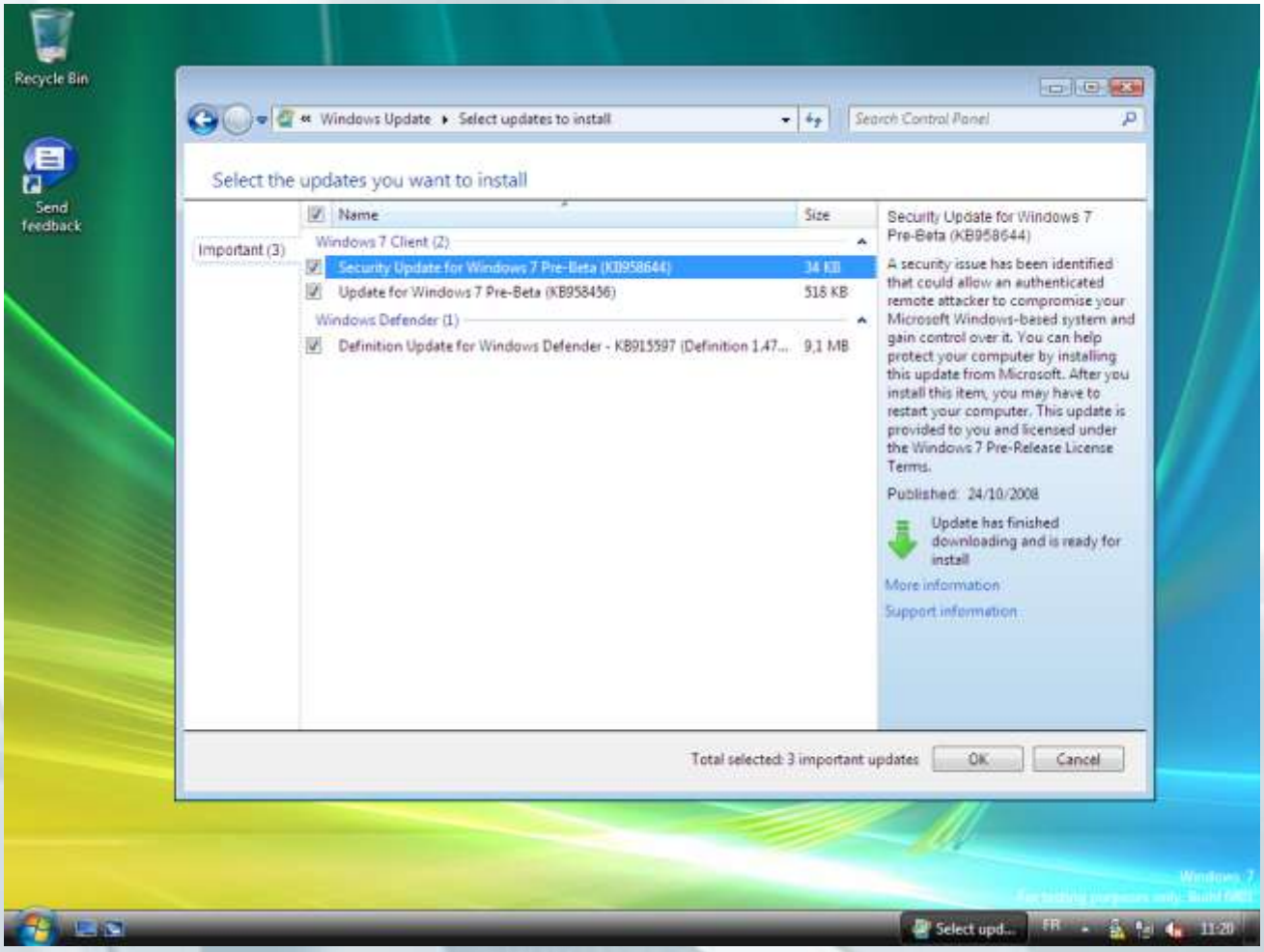
- ".NET Sploit"
  - Pour manipuler du code .NET dynamiquement
  - Point intéressant: le remplacement de librairies signées ... (slide #18)
  - http://www.applicationsecurity.co.il/english/NETFrameworkRootkits/tabid/161/Default.aspx
- OWASP "top 10" vs. Visual Studio
  - http://msdn.microsoft.com/en-us/library/dd129898.aspx
- Microsoft "Oslo"
  - Programmation *model-driven*
  - Langage "M"
  - http://msdn.microsoft.com/en-us/oslo/default.aspx
- Visual Studio 2010 sera entièrement en WPF
  - A noter également: fuite des symboles privés dans la CTP !
  - http://kobyk.wordpress.com/2008/10/29/oops-microsoft-private-symbols-accidently-leaked-in-visual-studio-2010-ctp-vm-image/

Infos Microsoft (6/9)

- Microsoft "Small Basic"
  - Pour faire tourner Nibbles.bas sur un *dual-core* ☺
  - http://msdn.microsoft.com/en-us/devlabs/cc950524.aspx
- Après le BluRay, la BluMouse
  - http://blogs.technet.com/mstechdays/archive/2008/12/01/une-souris-qui-fonctionne-sur-toutes-les-surfaces-m-me-les-plus-extr-mes.aspx
  - http://www.microsoft.com/france/chezvous/bluetrackproject/
- Windows Seven Developer's Guide
  - http://code.msdn.microsoft.com/Win7DeveloperGuide
- Windows Seven pourra émuler une carte vidéo compatible DirectX 10
  - Nom de code : WARP (Windows Advanced Rasterization Platform)
  - http://www.clubic.com/actualite-243462-microsoft-warp-jouez-crysis-graphique.html

Infos Microsoft (7/9)

- Déjà des mises à jour pour Windows Seven ☺



Infos Microsoft (8/9)

- Source: http://www.spamhaus.org/statistics/networks.lasso

The 10 Worst Spam Service ISPs		As at 23 November 2008
Rank	Network	Number of Current Known Spam Issues
1	cncgroup-hn	34
2	gilat.net	30
3	hostfresh.com	30
4	vsnlinternational.com	29
5	sistemnet.com.tr	27
6	microsoft.com	27
7	cnuninet.com	26
8	ecommerce.com	25
9	colocentral.com	24
10	xo.com	23

Infos Microsoft (9/9)

- **Une campagne de pub audacieuse au Canada**

Infos Microsoft (9/9)

- Microsoft va lancer une ligne de vêtements
  - http://www.boygeniusreport.com/2008/12/06/microsoft-prepares-to-launch-its-own-clothing-line-no-seriously/

Infos Réseau

- Sprint décide de ne plus router le trafic de Cogent
  - http://tech.slashdot.org/tech/08/10/31/0439245.shtml
  - http://www.earthtimes.org/articles/show/sprint-nextel-severs-its-internet-connection-to-cogent-communications,603138.shtml
- AS16735 (Brésil) décide de voler l'Internet mondial
  - http://www.renesys.com/blog/2008/11/brazil-leak-if-a-tree-falls-in.shtml
- Faille IOS
  - Paquet VTP malformé
    - http://www.cisco.com/warp/public/707/cisco-sr-20081105-vtp.shtml

Infos Réseau

- Plus de Mac == Plus d'IPv6
  - Accessoirement la France est 2ème mondial grâce à Free !
    - http://arstechnica.com/news.ars/post/20081113-google-more-macs-mean-higher-ipv6-usage-in-us.html
- IPv6 : +300% depuis 2 ans
    - http://www.nro.net/documents/press_release_031108.html
- NetWitness Investigator en version gratuite
    - http://download.netwitness.com/download.php?src=DIRECT

Infos Unix

- Failles
  - Serveur DHCP de Solaris 8 / 9 / 10 (CVE-2007-5365)
  - Xen Server 4.0.1 et 4.1.0
    - Faille dans le support ext2 permettant l'évasion du système invité
      - http://support.citrix.com/article/CTX118766
  - GnuTLS < 2.6.2
    - Un certificat autosigné peut être inséré dans une chaine de confiance
      - http://article.gmane.org/gmane.comp.encryption.gpg.gnutls.devel/3217
  - Protocole SSH (!)
    - Probabilité de 2^18 de récupérer 32 bits de *plaintext*
    - Cause: utilisation incorrecte du mode CBC
      - http://www.cpni.gov.uk/Docs/Vulnerability_Advisory_SSH.txt
    - Voir aussi
      - http://secunia.com/Advisories/32740/

Infos Unix

- Office 2007 -> OpenOffice, ça fonctionne
  - http://katana.oooninja.com/w/odf-converter-integrator
- Comment réussir ses présentations ?
  - http://impressive.sourceforge.net/
- La faille Debian/OpenSSL, de l'histoire ancienne ?
  - Pas vraiment ...
    - http://codefromthe70s.org/sslblacklist-badcerts.asp
  - On y trouve par exemple:
    - http://codefromthe70s.org/certcheck.asp?t=mail.gandi.net

Infos Unix

- Une régression dans Ubuntu / system-tools-backends
  - Les mots de passe repassent sur 8 caractères ☺
    - https://bugs.launchpad.net/ubuntu/+source/system-tools-backends/+bug/287134
    - http://www.ubuntu.com/usn/usn-663-1
- OpenBSD 4.4 "commence" à supporter les exécutables 100% PIE
- Une version alpha de Flash Player pour Linux et Solaris 64 bits
- Python 3.0 disponible
- Forum PHP 2008
  - 8 et 9 décembre
  - Il y aura un concours "hackez moi ça" ☺

Infos Unix

- Linus Torvalds vs. Apple Mac OS X: "this is utter crap"
  - Peut-être même pire que Vista ☺
    - http://www.smh.com.au/news/technology/utter-crap-torvalds-pans-apple/2008/02/05/1202090393959.html
- Apple recommande l'utilisation d'un antivirus ?
  - Une "erreur" : la note a été rapidement retirée
    - http://www.01net.com/editorial/397943/une-fois-n-est-pas-coutume-apple-recommande-un-antivirus-sur-mac/
    - http://www.heise-online.co.uk/security/Apple-recommend-anti-virus-software-Update-2--/news/112115
- Une nouvelle version du malware "DnsChanger" pour Mac OS X
    - http://isc.sans.org/diary.html?storyid=5390
- Une attaque DNS sur Android également ?
    - http://forums.t-mobile.com/tmbl/board/message?board.id=Android3&thread.id=19618

Failles

- Presque 1 an pour patcher une faille dans Acrobat Reader ?
  - Faille critique dans util.printf()
  - Découverte par ZDI, Secunia et Core
  - Note: la même faille affectait Foxit Reader !
    - http://expertmiami.blogspot.com/2008/11/adobe-acrobat-madness.html
    - http://sid.rstack.org/blog/index.php/303-adobe-vs-responsible-disclosure
  - Désormais largement exploitée dans la nature
    - http://blog.didierstevens.com/2008/11/10/shoulder-surfing-a-malicious-pdf-author/
- D'autres failles dans Acrobat ...
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=755
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=756
  - Et même le composant de mise à jour !
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=754
- Conclusion: mettre à jour en version 8.1.3 ou 9
    - http://www.adobe.com/support/security/bulletins/apsb08-19.html

Failles

- Et sinon ...
  - FireFox < 2.0.0.18 (11 failles), < 3.0.4
  - ThunderBird < 2.0.0.18
  - Opera <= 9.62
    - URL "file://" excessivement longue ...
  - Safari < 3.2 (11 failles)
    - http://support.apple.com/kb/HT3298
  - VLC < 0.9.7
  - Java < 1.6.11
  - Flash < 9.0.151.0
    - 6 failles corrigées
      - http://www.adobe.com/support/security/bulletins/apsb08-20.html
      - http://blogs.zdnet.com/security/?p=2130
    - Flash 10 n'est pas affecté
    - Mais Adobe AIR si !
      - http://www.adobe.com/support/security/bulletins/apsb08-23.html

Failles

- VMWare
  - Elévation de privilèges dans le *guest*
    - http://lists.vmware.com/pipermail/security-announce/2008/000042.html
  - Evasion *guest* vers *host*
    - Affecte: toutes versions sauf les dernières
      - VMWare Workstation 6.5, VMWare Server 2.x, etc.
    - http://lists.vmware.com/pipermail/security-announce/2008/000046.html

Failles

- Spoofing d'URL dans Google Chrome (désormais corrigé)
  - http://www.theregister.co.uk/2008/10/26/google_chrome_address_spoofing/
- Encore un *integer overflow* dans dns2tcp < 0.4.2 ☺
  - http://www.securityfocus.com/bid/32071/info
- iPhone 2.2 (12 failles)
  - http://blogs.zdnet.com/security/?p=2207

- Le mécanisme de signature Apple ne suit pas les liens symboliques
  - Donc une application iPhone signée peut inclure des parties dynamiques
    - http://collison.ie/blog/2008/11/dynamic-defaultpng-files-on-the-iphone

- En parlant d'iPhone ...
  - Linux pour iPhone
    - http://linuxoniphone.blogspot.com/
  - Déverrouiller l'iPhone avec style
    - http://news.cnet.com/8301-17938_105-10107580-1.html
  - Une connexion 3G un peu trop rapide
    - http://www.pcpro.co.uk/news/239556/what-the-banned-iphone-advert-should-really-look-like.html

Failles

- **WPA-TKIP est mal**
  - **Attaque AP vers station uniquement**
  - **Cadence de 1 octet par minute**
  - **Mais ça marche ...**
    - **http://arstechnica.com/articles/paedia/wpa-cracked.ars**
- **Metasploit 3.2 disponible**

Malwares et spam

- Des chercheurs infiltrent le réseau Storm Worm
  - 1,5% du réseau compromis
  - 350 millions de spams envoyés
  - 28 achats effectifs
  - Au final, un revenu annuel estimé à $3,5 millions
    - http://voices.washingtonpost.com/securityfix/2008/11/study_spam_still_profitable_at.html

- L'hébergeur McColo coupé du net
  - Affecte de manière significative la quantité de spam émis (50% à 75% !)
    - http://voices.washingtonpost.com/securityfix/2008/11/major_source_of_online_scams_a.html
    - http://voices.washingtonpost.com/securityfix/2008/11/spam_volumes_drop_by_23_after.html
  - Remarque: le fondateur de McColo était mort en septembre dans un accident de voiture à Moscou
    - http://www.tden.ru/articles/018047/

Malwares et spam

- EstDomains coupé depuis le 24 novembre 2008
  - http://www.icann.org/en/announcements/announcement-12nov08-en.htm
- Antivirus XP 2008 en lien sponsorisé sur Google
  - Un malware notoire !
    - http://www.dailytech.com/Google+Offers+Text+Ads+Linked+to+Malware+Site/article13436.htm
- Formalisation des principes de test antivirus
  - AMTSO = *Anti-Malware Testing Standards Organization*
    - http://www.amtso.org/documents/cat_view/13-amtso-principles-and-guidelines.html
- La crise économique, une aubaine pour les cyber-criminels ?
  - http://www.darkreading.com/security/attacks/showArticle.jhtml?articleID=211601123
- Un virus qui évite les ordinateurs Ukrainiens
  - http://www.microsoft.com/security/portal/Entry.aspx?Name=Worm%3aWin32%2fConficker.A

Malwares et spam

- Un malware qui installe un faux serveur DHCP sur sa victime
  - http://isc.sans.org/diary.php?storyid=5434
- Un CAPTCHA sans interaction humaine
  - http://pramana.com/
- Le rapport F-Secure pour S2 2008
  - Le nombre de souches explose (x3)
    - http://www.f-secure.com/2008/2/index.html

Failles 2.0

- Google corrige finalement la faille de téléchargement sans confirmation dans Chrome
  - http://blogs.zdnet.com/security/?p=2032
- Le téléphone Google Android a été "jailbreaké"
  - Un non évènement si on considère que c'est une plateforme "ouverte" ...
  - Mais la méthode est belle: telnet localhost ☺
  - Et l'explication est encore plus belle: tout ce qui est tapé à l'écran est envoyé dans un shell (!)
    - http://blogs.zdnet.com/Burnette/?p=680
    - http://code.google.com/p/android/issues/detail?id=1207
    - http://android-dls.com/forum/index.php?f=15&t=151&rb_v=viewtopic
- Google Native Client
  - Remplacer JavaScript par x86 ...
    - http://code.google.com/p/nativeclient/

Failles 2.0

- BrowserRider pour exploiter les failles des navigateurs
  - http://www.engineeringforfun.com/wiki/index.php/Browser_Rider
- Vinton Cerf
  - "Internet is free for all and every man for himself"
    - http://www.guardian.co.uk/technology/2008/oct/02/interviews.internet
- Crapto1 vs. MIFARE Classic
  - http://code.google.com/p/crapto1/
  - Voir également les numéros Linux Magazine et MISC Hors Série sur la carte à puce
- Des DDoS de 40 GB/s ?
  - Attention: étude du vendeur Arbor Networks
    - http://www.zdnet.fr/actualites/informatique/0,39040745,39384798,00.htm

Failles 2.0

- SeriousMagic.com victime d'une injection SQL automatisée
  - Ce site a récemment été racheté par Adobe
    - http://blogs.zdnet.com/security/?p=2039
- Un ver Facebook
  - Très "1.0": il se propage via un ".EXE" hébergé sur un site tiers
    - http://shiflett.org/blog/2008/nov/facebook-worm
- D-Link va un peu loin dans le marketing
    - http://www.ubersource.com/?p=17

Actualité (France)

- Les premiers certificats CSPN délivrés
  - http://www.ssi.gouv.fr/fr/confiance/certif-cspn.html
- "Sécurité Informatique" devient "Sécurité de l'Information"
  - http://www.sg.cnrs.fr/FSD/securite-systemes/revue.htm
- Elections prud'homales par Internet vs. Firefox 3
  - http://www.ecrans.fr/Elections-prud-homales-le-bug-du,5753.html
  - https://www.vote.prudhommes.gouv.fr/
- Elections prud'homales vs. liste d'émargement
  - http://eco.rue89.com/2008/11/27/prudhommes-le-vote-electronique-pourrait-etre-annule

Actualité (France)

- La CNIL rappelle à l'ordre un site mal protégé
  - A savoir: entreparticuliers.com
    - http://www.cnil.fr/index.php?id=2540&news[uid]=594
- Un (prochain) logiciel de sensibilisation en français
    - http://www.securite-informatique.gouv.fr/gp_article220.html
- Free assigné au tribunal pour violation de GPL
  - On va enfin savoir si le firmware de la Freebox est "distribué" aux utilisateurs – au sens de la GPL – ou pas
    - http://www.pcinpact.com/actu/news/47507-free-assigne-violation-licence-gpl.htm

Actualité (France)

- Une pub européenne pour sensibiliser à la sécurité
  - www.famille.gouv.fr
    - http://www.youtube.com/watch?v=cE6fQwWggVM
- Un nouvel entrant dans le domaine de "l'exploit privé"
  - Après WabiSabiLabi ...
  - Les vendeurs d'IDS/IPS vont finir par être à sec ☺
    - http://www.frsirt.com/exploits/
    - http://www.vupen.com/exploits-fr#offensive
- Une nouvelle conférence de sécurité française
    - http://www.frhack.org/

Actualité (France)

- La loi HADOPI fait des vagues
  - http://www.ca-va-couper.fr/
  - http://www.laquadrature.net/en/european-citizens-mobilize-block-sarkozys-graduated-response-council
- Le filtrage d'Internet en marche
  - http://www.degroupnews.com/actualite/n2994-internet-filtrage-fai-nadine_morano-michelle_alliot_marie.html
- La France est-elle vraiment championne du téléchargement illégal ?
  - Les chiffres sont sujet à caution
    - http://www.pcinpact.com/actu/news/47175-chiffre-piratage-milliard.htm
- Le portail PHAROS
  - "Dans un souci de préserver un espace où chacun peut communiquer, découvrir et s'épanouir (...)"
    - https://internet-signalement.gouv.fr/

Actualité (France)

- 1 million d'euros détournés par des bulgares
  - 2 lecteurs CB de stations service avaient été piégés
    - http://www.ouest-france.fr/actu/actuDet_-Un-million-retire-sur-des-comptes-de-l-Ouest-_3636-741400_actu.Htm

- Société Générale: "grâce à l'amélioration de notre système de contrôle interne, une fraude comme celle de Kerviel n'est plus possible"
    - http://afp.google.com/article/ALeqM5jEiHRRBqS7wyqiwGXTh6mOpfL_Kw

Actualité (USA)

- Google vs. Charlie Miller
  - Une faille (peu critique) trouvée dans Google Android le jour de sa sortie
  - Mais Google joue les méchants
    - http://news.cnet.com/8301-13739_3-10075488-46.html
    - http://ha.ckers.org/blog/20070817/xss-hole-in-google-apps-is-expected-behavior/
  - Voir aussi:
    - http://www.coresecurity.com/content/advisory-google

- Google crée son propre "standard" en marge d'OpenID 1.0
    - http://tech.slashdot.org/tech/08/10/29/2043218.shtml
  - Note: Microsoft s'est rangé à OpenID 1.0 ☺
    - http://it.slashdot.org/it/08/10/29/1328201.shtml?tid=109

- Suivre l'épidémie de grippe (aux USA) grâce à Google
    - http://www.google.org/flutrends/

- Google Chrome aura des plugins
    - http://dev.chromium.org/developers/design-documents/extensions

Actualité (USA)

- La Defense Intelligence Agency cesse d'utiliser un compteur de visites irlandais
  - http://www.informationweek.com/news/security/government/showArticle.jhtml?articleID=211800622
- Le DoD interdit les clés USB
  - Un virus se propage massivement par ce biais !
    - http://blog.wired.com/defense/2008/11/army-bans-usb-d.html
- La NASA victime d'attaques à répétition
  - http://www.businessweek.com/magazine/content/08_48/b4110072404167.htm
- Un employé Intel passe chez AMD
  - Intel estime le préjudice à 1 milliard de dollars !
    - http://www.networkworld.com/news/2008/110608-intel-trade-secrets-theft-indictment.html

Actualité (USA)

- Les emails de la Maison Blanche visités plusieurs fois par des hackers chinois
  - http://www.theregister.co.uk/2008/11/07/white_house_email_china/
- Obama et McCain piratés tous les deux !
  - http://www.newsweek.com/id/167581
- Encore "un coup des Chinois" ? ☺
  - http://www.courrierinternational.com/article.asp?obj_id=91897
  - La Chine dément
    - http://www.lemonde.fr/web/depeches/0,14-0,39-37677023@7-37,0.html
- Et maintenant "le coup des Russes"
  - http://www.latimes.com/news/nationworld/iraq/complete/la-na-cyberattack28-2008nov28,0,230046.story

Actualité (USA)

- Un site médical américain racketté
  - Les données personnelles des clients ont été volées
    - http://voices.washingtonpost.com/securityfix/2008/11/extortionists_target_major_pha.html
- Le système de contrôle des feux tricolores à Los Angeles piraté
    - http://www.vnunet.com/vnunet/news/2230263/los-angeles-engineers-pled
- Le vol de cuivre, une menace pour les infrastructures
    - http://infosecurity.us/?p=4079
- Le réseau du FMI piraté
    - http://www.theinquirer.fr/2008/11/16/un-pirate-sinvite-dans-le-reseau-informatique-du-fmi.html

Actualité (USA)

- Une plainte déposée pour faire "autopsier" les machines à voter
  - http://blogs.zdnet.com/security/?p=2119
- Les machines à voter violeraient également la GPL
  - http://arstechnica.com/news.ars/post/20081104-diebold-faces-gpl-infringement-lawsuit-over-voting-machines.html
- Un guide publié par l'EFF : comment faire de la recherche de failles aux USA
  - http://www.eff.org/issues/coders/grey-hat-guide

Actualité

- La Grande-Bretagne réfléchit à doter les PC des particuliers d'une "boite noire"
  - Installée chez les ISP
    - http://www.theinquirer.net/gb/inquirer/news/2008/11/07/british-government-spy
- L'Algérie réfléchit également à sa sécurité informatique
    - http://www.tsa-algerie.com/Securite-informatique---l-Algerie-va-se-doter-d-un-systeme-d_5306.html
- Europol reçoit 300,000 euros pour créer un trojan
    - http://news.cnet.com/8301-1009_3-10110133-83.html
- Une clé USB perdue en Grande-Bretagne
  - Contient les codes d'accès à un système de paiement en ligne utilisé par 12 millions de personnes
  - Perdue sur un parking de supermarché par un employé Atos
  - Retrouvée et envoyée au Daily Mail
    - http://www2.canoe.com/techno/nouvelles/archives/2008/11/20081104-081248.html

Actualité

- Les adresses IP des services secrets allemands (BND) dans la nature
  - Permet des corrélations intéressantes avec Google, Wikipedia, ...
    - http://wikileaks.org/wiki/German_Secret_Intelligence_Service_(BND)_T-Systems_network_assignments,_13_Nov_2008
    - Dont: www.belle-escort.de

- CERT/CC Resiliency Engineering Framework
    - http://www.cert.org/resiliency_engineering/framework.html
    - http://www.cert.org/archive/pdf/REFv0.95R_outline.pdf

- RSA publie son étude annuelle sur la sécurité des réseaux WiFi
  - Cibles: Paris, Londres et New York
    - http://www.rsa.com/node.aspx?id=3268

Actualité

- SHA-3 est en marche
  - http://131002.net/sha3lounge/
  - Parmi les candidats, MD6
    - http://groups.csail.mit.edu/cis/md6/
- BarsWF pour AMD est en marche
  - http://3.14.by/forum/viewtopic.php?f=8&t=37
- Les fichiers Acrobat 9 moins bien protégés qu'Acrobat 8
  - En cause : l'utilisation d'un simple SHA-256 pour dériver la clé de chiffrement AES-256
    - http://blogs.zdnet.com/security/?p=2271
- Forensics Oracle "offline" avec l'outil "CadFile"
  - http://www.databasesecurity.com/

Actualité

- **Du RFID pour détecter le vol de portables ?**
  - **Ca n'est pas la panacée ...**
    - **http://www.digitalidnews.com/2008/11/12/saving-the-dell-using-rfid-to-improve-laptop-security**

- **Lenovo invente le portable désactivable par SMS**
    - **http://www.itworld.com/hardware/58344/lenovo-service-disables-laptops-text-message**

- **Un homme arrêté par erreur**
  - **La carte SIM de son téléphone avait été clonée**
  - ***"The experts said no one has actually done any research on SIM card cloning because the activity is illegal in the country."***
    - **http://www.schneier.com/blog/archives/2008/11/the_ill_effects_1.html**

Actualité

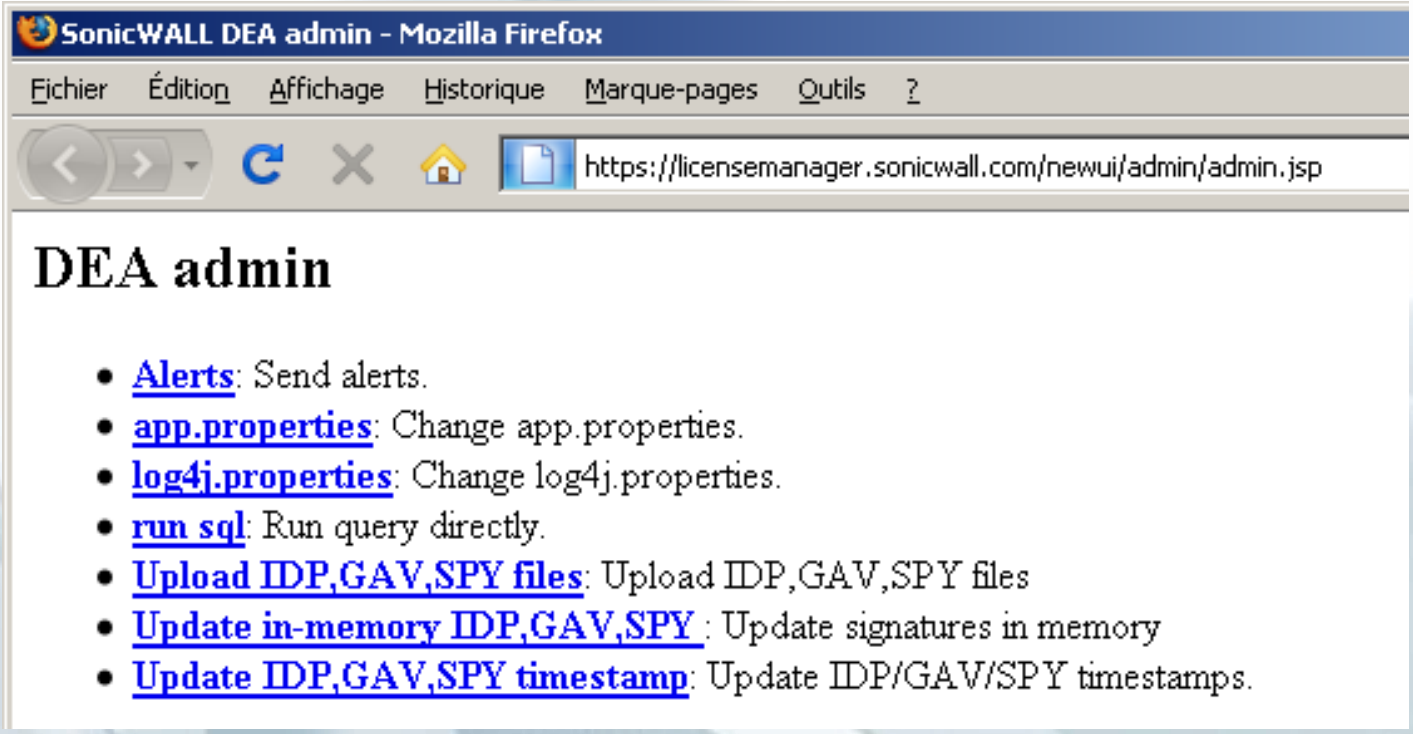
- Un système d'exploitation EAL6+ sur le marché
  - On ne peut pas encore payer ses impôts en ligne avec ☺
    - http://www.ghs.com/news/20081117_integrity_EAL6plus_security.html

- Le "Morris Worm" a 20 ans

Actualité

- **SonicWall (epic) fail**
  - **http://isc.sans.org/diary.html?storyid=5419**

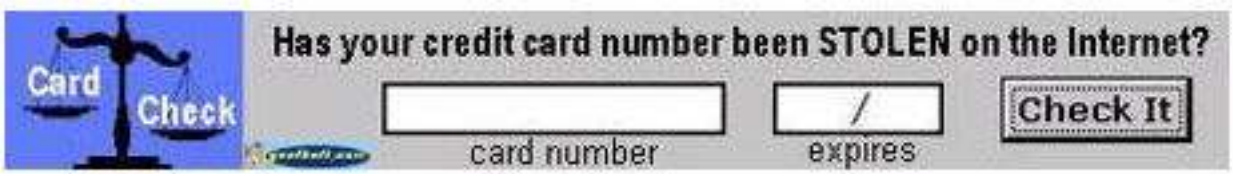
- **Et re-fail**



Fun

- Le buzz "cassoulet" a fonctionné
  - http://www.lepost.fr/article/2008/11/13/1324763_comment-le-mot-cassoulet-est-devenu-un-enorme-buzz-aux-etats-unis.html#xtor=AL-235
  - http://www.google.com/insights/search/#q=CASSOULET&geo=US&date=today%203-m&cmpt=q
- Un prisonnier "hack" sa prison
  - http://blogs.zdnet.com/projectfailures/?p=1158
- Reproduire une clé à partir d'une photo ... automatiquement
  - http://www.physorg.com/news144519246.html
- La fin d'un mythe sur le Luxembourg
  - http://www.cases.public.lu/fr/actualites/actualites/2008/11/19_SE/index.html
- The Matrix runs on Windows
  - http://www.collegehumor.com/video:1886349

Fun



- Source: http://failblog.org/

Questions / réponses

- Questions / réponses

- Assemblée générale de l'association (matin)
- Prochaine réunion (après-midi)

  - **Mardi 13 janvier 2008**

- N'hésitez pas à proposer des sujets et des salles