# OSSIR
# Groupe Paris

## Réunion du 4 novembre 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 (1/9)

- Correctifs de Octobre 2008 [avec *Exploitability Index*]
  - 1 = risque maximal, 3 = risque minimal
  - MS08-056 [2] Fuite d'information dans Office
    - Affecte : Office XP SP3
    - Exploit(s) : faille dans le support du protocole cdo://, conduisant à un XSS potentiel
      - Le correctif ne fait que supprimer l'association cdo://
    - Crédit :
      - NetAgent Co., Ltd.
  - MS08-057 [1/2/2] Failles dans l'interprétation du format XLS (x3)
    - Affecte : Excel (toutes versions supportées, y compris Excel pour Mac et Excel Viewer), SharePoint 2007
    - Exploit(s) : exécution de code à l'ouverture d'un fichier XLS malformé
      - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=746
    - Crédit :
      - Wushi / ZDI
      - Lionel d'Hauenens / LaboSkopia / iDefense
      - Joshua J. Drake / iDefense

# Avis Microsoft (2/9)

- MS08-058 [public/1/1/2/3/3] Patch cumulatif pour IE
  - Affecte : IE (toutes versions supportées)
  - Exploit(s) : corrige 6 failles, dont des violations de la politique de sécurité Cross-Domain et des accès à de la mémoire non initialisée
  - Crédit :
    - David Bloom
    - Gregory Rubin
    - Ivan Fratric / ZDI ( http://ifsec.blogspot.com/ )
    - Thierry Zoller / nRuns
    - Lee Dagon / Composica

- MS08-059 [1] Faille RPC dans le produit HIS
  - Affecte : Host Integration Server (toutes versions supportées)
  - Exploit(s) : exécution de code à distance
    - Appel RPC conduisant à un CreateProcess()
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=745
    - http://blogs.technet.com/swi/archive/2008/10/14/ms08-059-running-microsoft-host-integration-server-2006-as-non-admin.aspx
  - Crédit :
    - Stephen Fewer / Harmony Security / iDefense

# Avis Microsoft (3/9)

- MS08-060 [2] Faille critique dans Active Directory
  - Affecte : Windows 2000 SP4
  - Exploit(s) : exécution de code à distance via une requête LDAP malformée
  - Crédit :
    - Paul Miseiko / nCircle

- MS08-061 [1/1/3] Failles noyau (x3)
  - Affecte : Windows (toutes versions supportées)
  - Exploit(s) : élévation de privilèges
    - Exploitation plus facile sur les systèmes multi-processeurs
    - http://blogs.technet.com/swi/archive/2008/10/14/ms08-061-the-case-of-the-kernel-mode-double-fetch.aspx
  - Crédit :
    - Paul Caton / iShadow
    - Thomas Garnier / SkyRecon

# Avis Microsoft (4/9)

- **MS08-062 [1] Faille dans Internet Printing Service**
  - **Affecte : IIS (toutes versions supportées)**
  - **Exploit(s) :**
    - ***Integer overflow* dans le module IPP conduisant à une exécution de code à distance**
    - **Authentification requise**
    - **http://expertmiami.blogspot.com/2008/10/encore-un-coup-des-chinois.html**
  - **Crédit :**
    - **CERT/CC (attaque ciblée détectée dans la nature)**

- **MS08-063 [2] Faille SMB**
  - **Affecte : Windows (toutes versions supportées)**
  - **Exploit(s) :**
    - **Exécution de code à distance via un paquet SMB malformé**
    - **Authentification + droits d'écriture sur un partage requis (a priori)**
  - **Crédit :**
    - **Joshua Morin / Codenomicon**

# Avis Microsoft (5/9)

- **MS08-064 [2] Faille dans la gestion des VAD (*Virtual Address Description*) par le noyau**
  - **Affecte : Windows (toutes versions supportées)**
    - **Sauf Windows 2000**
  - **Exploit(s) : élévation de privilèges locale**
  - **Crédit :**
    - **N/D**

- **MS08-065 [3] Faille MSMQ (*Message Queuing*)**
  - **Affecte : Windows 2000 SP4**
  - **Exploit(s) :**
    - **Fuite d'information (exécution de code peu probable) à distance via un appel RPC malformé**
    - **http://blogs.technet.com/swi/archive/2008/10/14/ms08-065-exploitable-for-remote-code-execution.aspx**
  - **Crédit :**
    - **Anonymous / ZDI**

# Avis Microsoft (6/9)

- MS08-066 [1] Faille dans AFD.SYS (*Ancillary Function Driver*)
  - Affecte : Windows XP / 2003 (toutes versions supportées)
  - Exploit(s) : élévation de privilèges
    - http://blogs.technet.com/swi/archive/2008/10/14/ms08-066-how-to-correctly-validate-and-capture-user-mode-data.aspx
  - Crédit :
    - Fabien Le Mentec / SkyRecon

- Plus un correctif "out of band" (23 octobre)
  - MS08-067 Faille dans NETAPI32.DLL
    - Affecte : Windows (toutes versions supportées)
    - Exploit : exécution de code à distance via RPC anonyme
      - Prérequis: service de partages de fichiers/imprimantes
        - \\.\pipe\browser et \\.\pipe\server
      - http://blogs.technet.com/swi/archive/2008/10/23/More-detail-about-MS08-067.aspx
      - http://www.nynaeve.net/?p=226

# Avis Microsoft (7/9)

- A noter également
  - Mises à jour WSUS
    - http://support.microsoft.com/kb/894199
  - Mises à jour "non sécurité
    - http://technet.microsoft.com/en-us/wsus/bb466214.aspx

- Prévisions pour Novembre 2008

# Avis Microsoft (8/9)

- Advisories
  - Q958963
    - Publication d'un code d'exploitation fonctionnel pour MS08-067
  - Q956391
    - Mise à jour des "killbits" pour 3 ActiveX tierce partie
  - Q951306
    - Le "Token Kidnapping" s'annonce comme la faille la plus dure à patcher de tous les temps
      - http://blogs.technet.com/swi/archive/2008/10/13/service-isolation-explanation.aspx
      - http://blogs.iis.net/nazim/archive/2008/10/14/token-kidnapping-in-windows.aspx
      - http://blogs.technet.com/msrc/archive/2008/10/13/questions-about-microsoft-security-advisory-951306.aspx
    - Workarounds pour IIS 6 et IIS 7:
      - http://www.microsoft.com/technet/security/advisory/951306.mspx

# Avis Microsoft (9/9)

- Révisions
  - MS08-041
    - Version 2.0 : Snapshot Viewer pour Access est également affecté
    - Version 2.1 : ajout d'un lien vers Q957198
  - MS08-057
    - Version 1.1 : détection possible par SMS
  - MS08-058
    - Version 1.1 : correction de noms de clés et fichiers
  - MS08-059
    - Version 1.1 : effets de bord documentés dans Q956695
  - MS08-060
    - Version 1.1 : mise à jour de la liste des logiciels non vulnérables
  - MS08-062
    - Version 2.0 : Windows 2008 sur Itanium n'est pas vulnérable
    - Version 2.1 : le service d'impression tourne avec les privilèges SYSTEM
  - MS08-063
    - Version 1.1 : pas de redémarrage nécessaire sur Vista/2008, correction de noms de clés
  - MS08-064
    - Version 1.1 : correction du lien MSDN
  - MS08-065
    - Version 1.1 : ce correctif remplace MS07-065

# Infos Microsoft (1/2)

- Sorties logicielles
  - Vista SP2 Beta
    - http://www.neowin.net/news/main/08/10/24/vista-sp2-build-16489-released-to-testers
  - Windows Embedded Standard 2009

- Knowledge Base (sélection)
  - Q953835
    - Les membres du groupe "Network Operators" ne peuvent pas utiliser NETSH sous Vista/2008
  - Q954902
    - Authorization Manager met en cache (trop longtemps) les informations d'autorisation
  - Q957967
    - Un bug (non sécurité ?) dans Hyper-V
  - Q957909
    - Un hotfix post-SP1 pour Outlook 2007

# Infos Microsoft (2/2)

- Actualité
  - Windows "Cloud" s'appelle Windows Azure
    - http://www.microsoft.com/azure/default.mspx
  - Windows Seven avant fin 2009 ?
      - http://www.neowin.net/news/main/08/10/22/windows-7-to-rtm-within-a-year
    - Il sera disponible sur les Asus EEE PC
      - http://www.edbott.com/weblog/?p=2181
  - Security Intelligence Report, volume 5 (janvier -> juin 2008)
      - http://www.microsoft.com/security/portal/sir.aspx
  - Office 14 sera une application Web
    - http://news.cnet.com/8301-10805_3-10076883-75.html
  - Microsoft durcit les sanctions dans WGA
    - Maintenant le fond d'écran est supprimé
  - Et s'attire les foudres des Chinois
    - http://www.china.org.cn/china/national/2008-10/21/content_16646396.htm

# Infos Réseau

- Pas plus d'information sur "la" faille TCP (SockStress) lors de la conférence T2
  - Juste une démo qui montre que ça marche
  - Les détails seront publiés quand tout le monde aura corrigé ...

# Infos Unix

- Failles
  - CUPS, libXML2, libSPF2, OpenSSH portable, ...
  - sadmind (Solaris 8 et 9)
    - http://www.securityfocus.com/archive/1/archive/1/497311/100/0/threaded
- Debian, c'est pas des rigolos
  - http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=502959

# Failles

- **Divers ...**
  - **VLC <= 0.9.4 (pas de correctif)**
  - **WireShark < 1.0.4**
  - **Opera < 9.6.2**
  - **OpenOffice < 2.4.2**
- **Antivirus**
  - **Trend Micro Office Scan, F-Secure, ...**
- **Flash**
  - **Failles non corrigées dans toutes les versions < 10.0.12.36**
    - **http://www.adobe.com/support/security/bulletins/apsb08-18.html**
- **Sun Java Web Proxy**
  - **Affecte : 4.0 -> 4.0.7**
  - **Exploit : *heap overflow***
    - **http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=747**
- **Drivers WiFi Marvell**
  - **Utilisé par les points d'accès Linksys (ex. WAP4400N)**
    - **http://www.securityfocus.com/archive/1/497285**

# Failles

- Oracle Quarterly Patch
  - http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2008.html
    - Oracle Database (x9)
    - Oracle Application Server (x7)
    - Oracle Collaboration Suite (x1)
    - Oracle E-Business Suite and Applications (x5)
    - Oracle enterprise manager (x2)
    - Oracle PeopleSoft / JD Edwards Applications (x5)
    - Oracle Siebel (x6)
    - BEA Product Suite (x6)

# Malwares et spam

- Le *banker* "Nuclear Grabber / Haxdoor" revit sous le nom "Adrenaline"
  - Même prix : $3,000
- Panda Software invente le terme de *Crimeware as a Service* (CaaS)
- L'ICANN sur le point de résilier son accréditation à EstDomains
  - Un *registrar* impliqué dans de nombreuses affaires de *malware*
    - http://www.icann.org/en/announcements/announcement-2-29oct08-en.htm
- McAfee vs. CyberCrime
    - http://www.mcafee.com/us/about/corporate/fight_cybercrime/index.html

# Failles 2.0

- Les outils pour Webmaster de Google vont signaler les sites vulnérables
  - http://googlewebmastercentral.blogspot.com/2008/10/message-center-warnings-for-hackable.html
  - https://www.google.com/webmasters/tools
- WPA-PSK cassé (pour de vrai) ?
  - Attaque cryptanalytique sur la PMK
    - http://pacsec.jp/
- Exécution de code malveillant via des bogues CPU
  - http://conference.hackinthebox.org/hitbsecconf2008kl/?page_id=214
- Les claviers toujours vulnérables aux attaques TEMPEST
  - http://lasecwww.epfl.ch/keyboard/

# Failles 2.0

- **Un vilain XSS sur hotjobs.yahoo.com**
  - **http://www.theregister.co.uk/2008/10/27/yahoo_xss_vuln/**

# Failles 2.0

- Les téléphones portables, futurs botnets ?
  - Il reste malgré tout pas mal de contraintes techniques
    - http://www.silicon.fr/fr/news/2008/10/15/l_attaque_des_telephones_mobiles_zombies
- Les navigateurs Chrome et Firefox 3.1 embarquent désormais une API de géolocalisation
    - http://www.01net.com/editorial/394084/les-sites-web-vont-pouvoir-geolocaliser-leurs-internautes/
- Un bug dans un calculateur d'avion (?)
  - Du code ADA
  - Mais un bug dans les *spécifications* reste possible
    - http://www.journaldunet.com/solutions/intranet-extranet/analyse/aviation-la-defaillance-d-un-ordinateur-pose-des-questions-de-securite.shtml

# Actualité (France)

- Rapport de la CNIL
  - "La France en retard dans la lutte contre la cybercriminalité"
  - En cause: l'absence de loi anti-phishing
    - http://www.linformaticien.com/Actualit%C3%A9s/tabid/58/newsid496/5137/la-france-en-retard-dans-la-lutte-contre-la-cybercriminalite/Default.aspx
- Comment se protéger du filoutage ?
  - Il faut entrer les adresses réticulaires à la main !
    - http://www.securite-informatique.gouv.fr/gp_article44.html
- La loi HADOPI présentée "en urgence" devant le Parlement
    - http://www.ecrans.fr/Christine-Albanel-Tout-ca-c-est,5499.html
    - http://www.senat.fr/dossierleg/pjl07-405.html
- Le Sénat va-t-il installer un spyware sur chaque PC ?
    - http://www.numerama.com/magazine/11170-Le-Senat-veut-installer-un-spyware-sur-tous-les-ordinateurs.html

# Actualité (France)

- Le Plan Numérique 2012 dévoilé
  - Fortement orienté sécurité sur Internet
    - http://francenumerique2012.fr/
    - http://www.journaldunet.com/solutions/acteurs/actualite/plan-numerique-2012-la-cybersecurite-au-premier-plan.shtml
- P. Pailloux aux Assises de la Sécurité
  - "Que la communauté informatique cesse de se morfondre"
    - http://www.vnunet.fr/news/p_pailloux_dcssi_que_la_communaute_informatique_cesse_de_se_morfondre_-2029013
- Le compte bancaire du président piraté
  - Une attaque "opportuniste" ?
  - Les auteurs ont été appréhendés
    - http://tf1.lci.fr/infos/france/faits-divers/0,,4129385,00-on-a-pirate-le-compte-bancaire-de-sarkozy-.html

# Actualité (France)

- L'AFNIC publie une procédure d'arbitrage simplifiée
  - 250 euros HT seulement
    - https://predec.afnic.fr/
- Ils ne sont pas morts
    - http://www.hackerzvoice.net/

# Actualité (USA)

- Mafiaboy (aka Michael Calce) sort un livre
  - http://mafiaboybook.com/
- 10 ans de prison pour un DoS sur scientology.org
  - http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=009059338
- Des nouvelles de la "War on Terror"
  - Twitter considéré comme un outil de terroriste
    - http://www.breitbart.com/article.php?id=081025182242.js2g2op8
  - La pédo-pornographie est connectée au terrorisme
    - http://www.timesonline.co.uk/tol/news/uk/crime/article4959002.ece
- Le FBI souhaite plus de coopération internationale contre le cybercrime
  - http://www.datanews.be/fr/news/90-55-20683/le-fbi-s-attaque-au-cyber-crime-a-l-echelle-internationale.html

# Actualité (USA)

- Le spam comme outil de désinformation ?
  - http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9117657
  - http://www.votersuppression.net/
- Google passe au vert
  - http://www.lemondeinformatique.fr/actualites/lire-google-s-investit-dans-les-energies-renouvelables-27274.html
- Loic Lemeur licencie 1/3 du personnel de Seesmic
  - http://www.20minutes.fr/article/262196/crise-financiere-C-est-la-crise-Loic-Le-Meur-licencie-un-tiers-de-son-personnel.php
- Symantec va également licencier et sous-traiter
  - http://www.networkworld.com/news/2008/103108-seeing-tough-times-ahead-symantec.html?hpg1=bn

# Actualité

- Norme PCI 1.2 adopté
  - Remarque: WEP interdit après Juin 2010 (!)
    - http://securite.reseaux-telecoms.net/actualites/lire-les-standards-de-securite-pci-12-sur-les-cartes-bancaires-adoptes-18926-page-1.html
- "3D Secure"
  - La date de naissance bientôt obligatoire pour les paiements en ligne
    - http://www.01net.com/editorial/391917/la-date-de-naissance-nouveau-sesame-pour-regler-par-carte-bancaire
- La sécurité de l'information est également une affaire culturelle (d'après Cisco)
    - http://news.cnet.com/8301-1009_3-10054314-83.html
    - http://securite.reseaux-telecoms.net/actualites/lire-les-informaticiens-francais-champions-de-la-violation-des-regles-de-securite-19027.html

# Actualité

- **WabiSabiLabi pourrait fermer**
  - **Les "0day" seraient achetés et intégrés à l'IDS OneShield**
    - **http://pcworld.about.com/od/firewallswirelesssecurity/WabiSabiLabi-May-Close-0day-Au.htm**

- **VMWare acquière BlueLane (?)**
    - **http://fr.securityvibes.com/vmware-s-offre-blue-lane-buzz-222.html**

# Actualité

- **Une plate-forme européenne contre la cybercriminalité**
  - **http://www.journaldunet.com/solutions/breve/securite/32958/creation-d-une-plate-forme-europeenne-de-lutte-contre-la-cybercriminalite.shtml**
- **Revues du téléphone Google Android**
  - **http://online.wsj.com/article/SB122411880249138993.html**
  - **http://gizmodo.com/5062977/t+mobile-g1-google-android-phone-review**
  - **http://www.engadget.com/2008/10/16/t-mobile-g1-review-part-2-software-and-wrap-up/**
  - **http://blogs.zdnet.com/cell-phones/?p=179**
- **Remarque: Apple et Google ont prévu un *kill switch* pour les applications "indésirables"**
  - **http://gizmodo.com/5064357/google-has-a-remote-kill-switch-for-android-apps**

# Fun

- Se protéger contre CookieMonster avec NoScript
  - http://security4all.blogspot.com/2008/10/use-noscript-to-force-websites-to-ssl.html
- Réactiver le support des certificats SSL autosignés dans Firefox
  - Attention: ceci n'est évidemment pas recommandé ☺
    - http://kuix.de/sslhazard/sslhazard.php
- Transformer son téléphone 3G en hotspot WiFi mobile ?
  - http://www.joikusoft.com/

# Questions / réponses

- Questions / réponses
- Prochaine réunion le mardi 9 décembre 2008
- N'hésitez pas à proposer des sujets et des salles