OSSIR
Groupe Sécurité Windows

Réunion du 8 octobre 2007

Revue des dernières vulnérabilités Microsoft

Cette veille est réalisée par les coanimateurs du groupe Windows

EdelWeb

Olivier REVENU
olivier.revenu (à) edelweb.fr

Mickaël DEWAELE
mickael.dewaele (à) edelweb.fr

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

Dernières vulnérabilités
Avis Microsoft (1/5)

- **Préalable**
  - La criticité indiquée pour chaque avis est donnée selon l'échelle Microsoft, à savoir
    - Faible
      - Une vulnérabilité dont l'exploitation est très difficile ou dont l'impact est minimale
    - Modéré
      - L'exploitabilité est limitée par des facteurs comme la configuration par défaut non vulnérable ou est très difficile à réaliser
    - Important
      - Une vulnérabilité dont l'exploitation aura pour impact l'atteinte à la confidentialité, l'intégrité ou la disponibilité des données des utilisateurs, voir l'intégrité ou la disponibilité du système
    - Critique
      - Une vulnérabilité dont l'exploitation peut permettre la propagation d'un vers Internet sans action de l'utilisateur
  - Les exploits indiqués pour chaque avis sont ceux connus publiquement à la date de cette présentation
  - Les systèmes affectés sauf mention contraire correspondent aux versions (Service Pack) actuellement supportées par l'éditeur

Dernières vulnérabilités
Avis Microsoft (2/5)

- **Correctifs de Septembre 2007**

  - **MS07-051 Faille dans Microsoft Agent**
    - **Affecte : Windows 2000 SP4**
    - **Exploit : "buffer overflow" lors du traitement d'une URL trop longue**
    - **Crédit : triple découverte**
      - **Assurent Secure Technologies**
      - **Yamata Li / Palo Alto Networks**
      - **iDefense**

  - **MS07-052 Faille dans Crystal Reports**
    - **Affecte : Visual Studio (toutes versions supportées)**
    - **Exploit : fichier RPT malformé**
    - **Crédit : n/d**

Dernières vulnérabilités
Avis Microsoft (3/5)

- **MS07-053 Faille dans Services For Unix**
  - **Affecte : SFU 3.0 et 3.5, sous-système POSIX**
  - **Exploit : élévation de privilèges via un fichier *setuid***
  - **Crédit : Brian A. Reiter / WolfeReiter**

- **MS07-054 Faille dans MSN Messenger**
  - **Affecte : toutes versions supportées sauf 7.0.0820 et 8.1**
  - **Exploit : exécution de code lors du démarrage d'un chat vidéo**
  - **Crédit : Woo Shi / team 509**

Dernières vulnérabilités
Avis Microsoft (4/5)

- **Prévisions pour Octobre 2007**
  - **5 bulletins critiques pour Windows (nécessitant un redémarrage)**
  - **1 bulletin critique pour Office**
  - **1 bulletin important pour Office et Windows**

Dernières vulnérabilités
Avis Microsoft (5/5)

- Advisories
  - N/A

- Révisions
  - MS07-042 Faille MSXML
    - Version 2.0 : ajout du pack de compatibilité Office 2007 + MSXML 4 sur Vista dans la liste des applications affectées
  - MS07-047 Faille Windows Media Player
    - Version 1.2 : précisions sur l'installation "unattended"
  - MS07-051 Faille Microsoft Agent
    - Version 1.1 : explication sur le fait que Windows XP n'est pas affecté
  - MS07-052 Faille Visual Studio
    - Version 1.1 : mise à jour du nom du correctif
  - MS07-053
    - Version 1.1 : détection par SMS 2003
  - MS07-054 Faille MSN Messenger
    - Version 1.1 : liens vers la mise à jour MSN Messenger 8.1

Dernières vulnérabilités
Infos Microsoft (1/8) - sorties

- Sorties logicielles
  - Betas et CTP
    - .NET 3.5 Beta2
    - Visual Studio 2008 Beta2
    - Deployment 4 Beta 3 (BDD 2007)
    - Windows Server 2008 RC0 (avec hyperviseur Viridian)
    - Windows Vista SP1 Beta (24 septembre)
  - Office 2003 SP3 : des changements de fond
    - Blocage des formats inusités
      - Cf. Q938810
      - Ex. Corel, PowerPoint 95
    - Blocage de composants COM spécifiques
      - Cf. Q938814, Q938815
  - SharePoint 2003 SP3
  - Project Server 2003 SP3

Dernières vulnérabilités
Infos Microsoft (2/8) - sorties

- Microsoft Application Verifier 3.4
- Process Explorer 11 (avec support Vista)
- Animations 3D pour Excel 2007
  - http://www.microsoft.com/downloads/details.aspx?FamilyID=D06CA9BF-CDC5-4253-B847-1139C5ED2575&displaylang=en
- Internet Explorer 7 désormais sans WGA
  - http://blogs.msdn.com/ie/archive/2007/10/04/internet-explorer-7-update.aspx

- **Sorties annoncées**
  - Windows Server 2008, SQL Server 2008, Visual Studio 2008
    - Q1 2008

- **Fin de support**
  - N/A

Dernières vulnérabilités
Infos Microsoft (3/8) - sorties

- Les 14 projets secrets de Microsoft
  - http://www.01net.com/editorial/359465/les-quatorze-projets-secrets-de-microsoft/
  - Halo 3 (sur XBox)
  - Live Search 2.0
  - Windows Home Server
  - Zune 2
    - http://www.microsoft.com/presspass/press/2007/oct07/10-02ZuneNextGenPR.mspx?rss_fdn=Press%20Releases
  - Internet TV
  - Windows Live TV
  - SharedView (travail collaboratif)
  - Works On Cloud (applications bureautiques en mode Web)
  - Surface, Kitchen PC, …
  - Windows Mobile 8.0
  - Viridian (hyperviseur)
  - Vista R2
  - XBox 3
  - Windows 7.0 (2010)

Dernières vulnérabilités
Infos Microsoft (4/8) - sécurité

- SiteLock
  - Un template pour "verrouiller" les contrôles ActiveX sur un site donné
  - http://www.microsoft.com/downloads/details.aspx?FamilyID=43cd7e1e-5719-45c0-88d9-ec9ea7fefbcb&displaylang=en

- Magazine "Uninformed" Volume 8
  - http://uninformed.org/
  - TOC :
    - S'échapper du mode protégé dans IE 7 sur Vista
    - Contourner PatchGuard v3
    - Un catalogue des backdoors noyau dans Windows
    - Etc.

- Le blog "hackers" devient "%41%43%45%20%54%65%61%6d"
  - http://blogs.msdn.com/hackers/

Dernières vulnérabilités
Infos Microsoft (5/8) - actualité

- Un système de "watermaking" audio inviolable chez Microsoft ?
  - http://www.informationweek.com/blog/main/archives/2007/09/microsoft_appli.html
- Mise à jour du client Windows Update sans confirmation utilisateur
  - http://windowssecrets.com/2007/09/13/01-Microsoft-updates-Windows-without-users-consent
- Black Screen of Darkness sous Vista
  - http://www.computerworld.com.au/index.php/id;1029262671;fp;16;fpid;1
- Comment contourner le Microsoft Fingerprint Reader avec de la Patafix
  - http://www.dailymotion.com/video/x3316e_fingerprint-reader-ms-bypass
- Microsoft achèterait 5% de FaceBook
  - http://www.linformaticien.com/Actualit%E9s/tabid/58/newsid496/2979/Microsoft-entrerait-dans-le-capital-de-Facebook/Default.aspx
  - La société est valorisée … 10 milliards de dollars !

Dernières vulnérabilités
Infos Microsoft (6/8) - actualité

- Bluehat le 27 et 28 septembre 2007
  - http://blogs.technet.com/msrc/archive/2007/09/20/announcing-bluehat-v6.aspx
  - Pas de vidéo pour l'instant, mais l'audio est disponible
    - http://blogs.msdn.com/michael_howard/archive/2007/10/04/bluehat-audio-available.aspx

- La "migration" IIS 7.0 du site microsoft.com
  - http://blogs.technet.com/mscom/archive/2007/09/07/the-tasty-morsels-found-in-dogfood-mscom-ops-top-10-changes-in-iis7-0.aspx

- Programme du Technet 2008 Disponible
  - http://blogs.technet.com/longhorn/archive/2007/09/27/les-nouveaux-s-minaires-technet-sont-arriv-s.aspx

- Microsoft et le Jéricho Forum
  - http://www.microsoft.com/technet/community/columns/secmgmt/sm0907.mspx

Dernières vulnérabilités
Infos Microsoft (7/8) - actualité

- Un article technique intéressant : "time based blind SQL injection"
  - http://www.microsoft.com/technet/community/columns/secmvp/sv0907.mspx
- Les arguments "de vente" de la virtualisation chez Microsoft
  - http://blogs.technet.com/fabricem_blogs/archive/2007/09/26/comparatif-prix-virtualisation-microsoft-vs-vmware.aspx
- Virtualisation et rootkits
  - http://www.microsoft.com/whdc/system/platform/virtual/CPUVirtExt.mspx
  - Des arguments … plutôt fumeux (cf. analyse sur Daily Dave)
- Code source du Framework .Net 3.5 (partiellement) publié avec VS 2008
  - http://weblogs.asp.net/scottgu/archive/2007/10/03/releasing-the-source-code-for-the-net-framework-libraries.aspx

Dernières vulnérabilités
Infos Microsoft (8/8) - Vista

- Les gadgets Vista, source de XSS
  - http://www.portcullis-security.com/uplds/Next_Generation_malware.pdf
- Vista progresse à 4,5% (en juin), Mac OS X reste à 6%
  - Mesuré sur les connexions Web
    - http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9027558
- Vista brûle 8 fois plus les disques de portables que XP
  - http://4sysops.com/archives/vista-burns-laptop-hard-disks-failure-eight-times-higher-than-under-xp/
- Windows Vista : 4 téléchargements améliorent vitesse et stabilité
  - http://www.silicon.fr/fr/silicon/news/2007/10/04/windows-vista-microsoft-am

Dernières vulnérabilités
Autres avis (1/9) – failles

- Failles "non sécurité" dans Excel
  - Excel 2003
    - http://www.pcinpact.com/actu/news/39215-excel-2003-bug-affichage-series-incrementati.htm
  - Excel 2007
    - http://www.pcinpact.com/actu/news/39085-excel-2007-bug-850-771.htm

- Java 6 Update 3
  - A priori pas de correctifs de sécurité
  - Mais propose d'installer OpenOffice !

Dernières vulnérabilités
Autres avis (2/9) – failles

- La saga des failles QuickTime
  - "Heap overflow" sur iTunes < 7.4
    - https://www.isecpartners.com/advisories/2007-005-itunes.txt
  - Exécution de code via le plugin FireFox
    - http://www.gnucitizen.org/blog/0day-quicktime-pwns-firefox
    - http://www.milw0rm.com/exploits/4399
    - Corrigé en quelques jours par Mozilla

- Faille critique dans Adobe Acrobat Reader
  - Exécution de code via un fichier PDF
    - Fiable (sans "buffer overflow")
  - http://www.gnucitizen.org/blog/0day-pdf-pwns-windows
  - http://www.youtube.com/watch?v=R_mv49Sdeok

Dernières vulnérabilités
Autres avis (3/9) – failles

- Faille dans MFC 4.2 et 7.1
  - "Heap overflow" dans CFileFind::FindFile
  - http://goodfellas.shellcode.com.ar/own/VULWKU200706142
  - Publié 3 mois après la notification à Microsoft

- Attaques XSIO : "Cross Site Image Overlaying"
  - http://www.disenchant.ch/blog/wp-content/uploads/2007/09/xsio.pdf
  - Placement astucieux d'images en superposition
  - Pas de script

- Faille(s) AIM
  - Dont une non corrigée à ce jour :
    - http://aviv.raffon.net/2007/09/25/ReadyAIMFire.aspx

- Mise à jour 1.1.1 pour l'iPhone
  - Corrige plusieurs failles critiques
  - Mais incompatible avec les téléphones "débloqués"…

Dernières vulnérabilités
Autres avis (4/9) – malware et spam

- Spam : les nouveautés du mois
  - Le spam 3D
  - Le spam se met au SPF
    - http://blogs.msdn.com/tzink/archive/2007/09/07/found-some-spammers-today-with-spf-records-set-up.aspx
- Un nouveau "ver" Skype
  - http://heartbeat.skype.com/2007/09/the_worm_that_affects_skype_fo.html
  - Ver IM "classique": se propage en envoyant des messages aux contacts
- Les virus se mettent au spoofing ARP !
  - http://www.avertlabs.com/research/blog/index.php/2007/09/18/web-page-code-injection-via-arp-spoofing/
- Le code source du trojan Shark2 à vendre chez son concurrent (XHacker)
  - Il a été volé … grâce à un trojan !
- Une "emergency blocklist"
  - http://threatstop.com/

Dernières vulnérabilités
Autres avis (5/9) – malware et spam

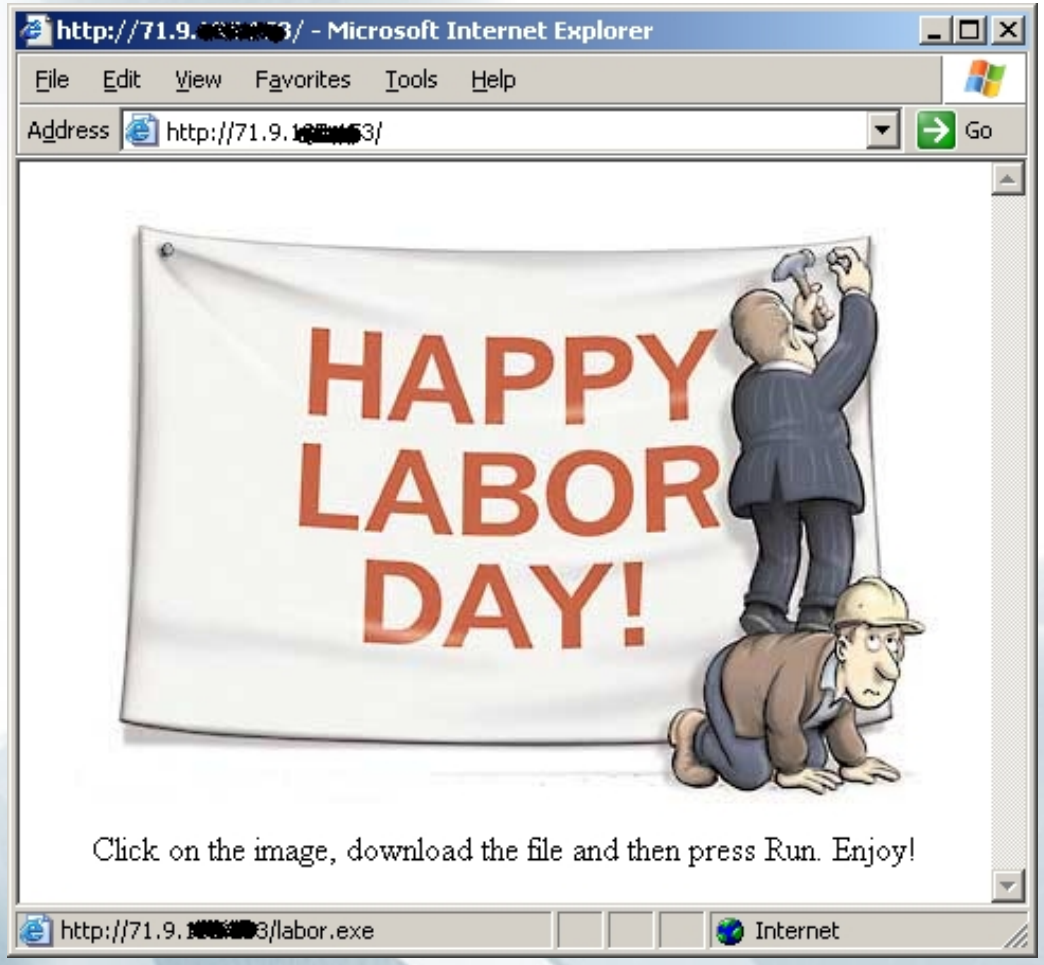
- Symantec pour les "whitelists" de binaires
  - http://www.cbc.ca/news/background/tech/privacy/white-list.html
  - C'est la position de Joanna Rutkowska également
- Encore une affaire de rootkit
  - Dans le jeu BioShock
    - http://www.avertlabs.com/research/blog/index.php/2007/08/24/digital-reality-misunderstanding/
- Google pénétré par les Chinois, info ou intox ?
  - http://www.googlewatchdog.info/2007/09/spam-and-virus-sites-infesting-google.html
  - A priori un simple empoisonnement de l'algorithme d'indexation

Dernières vulnérabilités
Autres avis (6/9) – malware et spam

- Les auteurs du virus "Fujack" arrêtés en Chine
  - Relativement exceptionnel …
  - http://www.avertlabs.com/research/blog/index.php/2007/08/23/fujacks-authors-face-charges-in-chinese-court/
- Les auteurs de "Downloader-AAP" arrêtés en Allemagne
  - http://www.avertlabs.com/research/blog/index.php/2007/09/13/the-end-of-downloader-aap/
- Un Californien arrêté : il dirigeait un botnet de 7000 machines
  - http://www.securityfocus.com/brief/601
- 77 arrestations dans une opération "anti scam"
  - Le montant de la fraude pourrait s'élever à 2 milliards de dollars
  - http://www.eweek.com/article2/0,1759,2191861,00.asp

Dernières vulnérabilités
Autres avis (7/9) – malware et spam

- Vous cliquez ?



Dernières vulnérabilités
Autres avis (8/9) – attaques 2.0

- Faille de redirection permanente dans GMail
  - http://www.gnucitizen.org/blog/google-gmail-e-mail-hijack-technique/
  - Rapidement corrigée
- Faille énorme sur le site d'Adobe
  - http://www.01net.com/editorial/360028/une-faille-de-securite-sur-le-site-d-adobe/
  - Un simple ".."dans l'URL …
- La coupe du monde de Rugby attire les pirates turcs …
  - http://www.zataz.com/news/14980/
- Le site de "Bank of India" sévèrement compromis
  - http://sunbeltblog.blogspot.com/2007/08/breaking-bank-of-india-seriously.html

Dernières vulnérabilités
Autres avis (9/9) – attaques 2.0

- La Chine se plaint d'être victime de cyber-attaques …
  - http://www.reuters.com/article/internetNews/idUSPEK8648420070912
- DidTheyReadIt.com
  - Pourquoi espionner du mail quand on peut le demander ?
- Facebook.fr n'est plus à vendre
  - http://fr.techcrunch.com/2007/10/02/facebookfr-quelquun-cherche-les-ennuis/
- 1727 entreprises françaises "agressées économiquement" selon les RG
  - http://www.capital.fr/actualite/Default.asp?indiscretion=1&numero=65332&Cat=IND

Dernières vulnérabilités
Autres infos (1/6) – just for fun

- L'ensemble des mails et du code source de la société Media Defender sur … BitTorrent
  - http://torrentfreak.com/mediadefender-emails-leaked-070915/
- Du coup, "The Pirate Bay" poursuit les majors pour hacking !
  - http://thepiratebay.org/blog/86
- Des données américaines confidentielles sur les réseaux P2P
  - http://computerworld.com/action/article.do?command=viewArticleBasic&articleId=9027949
- Un brevet anti-P2P à vendre …
  - … 1 million de dollars sur eBay !
  - http://cgi.ebay.com/ws/eBayISAPI.dll?ViewItem&rd=1&item=280156640645
- La chasse aux "trackers" continue
  - http://torrentfreak.com/mpaa-takes-down-isohunt-podtropolis-torrentbox-070925/
  - http://torrentfreak.com/demonoid-shut-down-by-cria-070925/

Dernières vulnérabilités
Autres infos (2/6) – just for fun

- Les jouets télécommandés "screenés" dans les aéroports américains
  - http://www.cnn.com/2007/TRAVEL/10/01/tsa.toys/index.html
- Le monde est-il plus sûr maintenant ?
  - http://www.symantecendpointgame.com/
- Les hackers sont à bonne école
  - iHack 2007
    - http://www.f-secure.com/weblog/archives/archive-082007.html#00001254
  - Hackers' Dojo
    - http://blog.wired.com/27bstroke6/2007/08/a-look-inside-a.html
  - Un "Kit de Hacking"pour $55
    - http://kit.hackerscenter.com/

Dernières vulnérabilités
Autres infos (3/6) – just for fun

- Francis Ford Coppola se fait voler son laptop
  - Avec une copie unique du script de son dernier film
    - http://www.nydailynews.com/gossip/2007/09/28/2007-09-28_francis_ford_coppolas_laptop_stolen.html
- Le Mac, trop convivial ?
  - Un voleur uploade par mégarde des photos de lui sur Flickr
    - http://www.boingboing.net/2007/09/24/idiot-criminal-uploa.html
- Google accusé de crime contre l'humanité
  - http://www.zataz.com/news/15124/Jayne-v.-Google-Internet-Search-Engine-Founders.html
- Les boucles bouclés de la sécurité ☺
  - http://www.securitymetrics.org/content/Wiki.jsp?page=Welcome_blogentry_061005_1

Dernières vulnérabilités
Autres infos (4/6) – just for fun

- Canular : un étudiant indien affirme glisser 256 Go sur une... feuille de papier!
  - http://www.silicon.fr/fr/silicon/news/2006/11/27/450-go-une-feuille-de-papier
- La technologie RFID utilisée pour commander son MacDo
  - http://www.journaldugeek.com/?2007/09/17/8617-pour-les-geeks-affames
- Arxceo Ally IP100 : boitier compact anti-hacker!
  - http://www.lindy.com/fr/productfolder/03/32/32459/index.php

Dernières vulnérabilités
Autres infos (5/6)

- **Fusions et acquisitions**
  - **Huawei rachète 3Com et TippingPoint / ZDI pour 2 milliards de dollars**
    - **http://blogs.zdnet.com/security/?p=549**
  - **eBay a du mal à digérer Skype**
    - **http://www.silicon.fr/fr/silicon/news/2007/10/02/ebay-tracass-l-acquisition-de**

Dernières vulnérabilités
Autres infos (6/6)

- **Et pendant ce temps là sur la mailing liste de l'OSSIR**
  - **Liste SUR**
    - **XSS et Sympa**
    - **Domainkey et DKIM**
    - **Création de l'OSSIR Bretagne**
  - **Liste NT**
    - **Un antivirus libre pour Windows**
    - **Le SPAM varie ses méthodes mais pour quel but ...**

Questions / réponses

- Questions / réponses
- Date de la prochaine réunion
  - Prochaine réunion le 12 novembre 2007
- N'hésitez pas à proposer des sujets et des salles