OSSIR
Groupe Sécurité Windows

Réunion du 9 juillet 2007

Revue des dernières vulnérabilités Microsoft

Cette veille est réalisée par les coanimateurs du groupe Windows

EdelWeb

Olivier REVENU
EdelWeb
olivier.revenu (à) edelweb.fr

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

Dernières vulnérabilités
Avis Microsoft (1/7)

- **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 (2/7)

- **Correctifs de Juin 2007**

  - **MS07-030 Vulnérabilité dans Visio**
    - **Affecte : Visio 2002 SP2, Visio 2003 SP2**
    - **Exploit : 2 failles exploitables via un fichier .VSD, VSS ou .VST**
    - **Crédit : Chris Ries / Vigilant Minds**

  - **MS07-031 Faille dans SCHANNEL**
    - **Affecte : Windows toutes versions supportées, sauf Vista**
    - **Exploit : *buffer overflow* dans le traitement des réponses SSLv3**
      - **http://www.sabre-security.com/files/schannel.swf**
    - **Crédit : Thomas Lim / COSEINC**

Dernières vulnérabilités
Avis Microsoft (3/7)

- **MS07-032 Fuite d'information dans Vista**
  - **Affecte : Vista**
  - **Exploit : un utilisateur non-administrateur peut lire des fichiers et des clés de base de registre accessibles aux administrateurs uniquement**
  - **Crédit : Robbie Sohlman**

- **MS07-033 Mise à jour cumulative pour IE**
  - **Affecte : Windows toutes versions supportées, y compris Vista**
  - **Exploit : corrige 6 failles, dont :**
    - **Instanciation de composants COM non destinés à être chargés dans IE**
    - ***Buffer overflow* dans le traitement d'un tag CSS**
    - ***Buffer overflow* à l'installation d'un pack de langue**
    - ***Buffer overflow* dans Speech API 4**
    - ***Spoofing* de site Web via la page "navigation annulée"**
  - **Crédit : iDefense, Tom Cross / ISS, Sam Thomas / ZDI, Will Dorman / CERT/CC, cocoruder / Fortinet**

Dernières vulnérabilités
Avis Microsoft (4/7)

- MS07-034 Mise à jour cumulative pour Outlook Express (et Windows Mail)
  - Affecte : Windows toutes versions supportées, y compris Vista
  - Exploit : 4 vulnérabilités, dont :
    - 3 fuites d'information
      - Ex. contournement de la Same Origin Policy via un tag "mhtml://"
    - Exécution de code via un lien "file://" vers un répertoire et un exécutable de même nom
      - Présentée en avril à l'OSSIR
  - Crédit : SANS ISC, Yosuke Hasegawa / WebAppSec.JP

- MS07-035 Vulnérabilité dans l'API Win32
  - Affecte : Windows toutes versions supportées, sauf Vista
  - Exploit : API LZOpenFile(), LZCreateFile()
  - Crédit : Billy Rios / VeriSign

Dernières vulnérabilités
Avis Microsoft (5/7)

- **Juillet 2007**
  - **Bulletin #1 (critique)**
    - **Affecte : Excel, toutes versions supportées (2000 -> 2007)**
    - **Exploit : exécution de code "à distance"**
  - **Bulletin #5 (critique)**
    - **Affecte : Windows, toutes versions supportées (2000 -> Vista, 32 et 64 bits)**
      - **En fait ".NET Framework" 1.0 -> 2.0**
    - **Exploit : exécution de code "à distance"**
  - **Bulletin #4 (critique)**
    - **Affecte : Windows 2000 Server, Windows 2003**
    - **Exploit : exécution de code "à distance"**

Dernières vulnérabilités
Avis Microsoft (6/7)

- **Bulletin #2 (important)**
  - **Affecte : Publisher 2007**
  - **Exploit : exécution de code "à distance"**
- **Bulletin #6 (important)**
  - **Affecte : Windows XP SP2**
  - **Exploit : exécution de code "à distance"**
- **Bulletin #3 (modéré)**
  - **Affecte : Vista 32 et 64 bits**
  - **Exploit : fuite d'information**

Dernières vulnérabilités
Avis Microsoft (7/7)

- Advisories
  - Aucun
- Révisions
  - MS07-022
    - Version 2.0 (re-release) : incompatibilité avec Windows 2000 SP4 sur les PC de type "NEC 98"
  - MS07-033
    - Version 1.2 : correction de la clé de base de registre à vérifier
  - MS07-034
    - Version 1.3 : ajout d'un lien vers Q929123

Dernières vulnérabilités
Infos Microsoft (1/5)

- OneCare obtient le VB Award 100%
  - http://www.appscout.com/2007/06/onecare_bounces_back.php
- Là où Kaspersky échoue …
  - http://community.zdnet.co.uk/blog/0,1000000567,10005452o-2000331828b,00.htm
- Le MSRC : l'un des 10 pires endroits où travailler
  - http://www.popsci.com/popsci/science/0203101256a23110vgnvcm1000004eecbccdrcrd.html
- Retour d'expérience sur la faille "DNS SRV"
  - http://blogs.msdn.com/sdl/archive/2007/06/28/lessons-learned-from-ms07-029-the-dns-rpc-interface-buffer-overrun.aspx
- Est-ce un phishing ???
  - http://www.microsoft.com/protect/yourself/password/checker.mspx

Dernières vulnérabilités
Infos Microsoft (2/5)

- La version Windows Server 2008 "Core" intégrera IIS 7.0
  - Mais sans ASP.NET car .NET Framework n'est pas intégré
- "www.microsoft.com" est passé sous IIS 7
  - http://uptime.netcraft.com/up/graph?site=www.microsoft.com
- "microsoft.co.uk" piraté via une injection SQL
  - http://www.zone-h.org/content/view/14780/31/
- Microsoft attaqué en justice par Google sur leur outil de recherche de bureau
- Les TechDays 2008 sont déjà annoncés
  - Du 11 au 13 février 2008

Dernières vulnérabilités Infos Microsoft (3/5)

- **Sorties logicielles**
  - Windows Home Server RC
  - Virtual Server 2005 R2 SP1
  - ISA Server 2004 SP3
  - Windows SteadyState
    - Ex. "Microsoft Shared Computer Toolkit"
  - Microsoft Diagnostics and Recovery Toolset
    - Ensemble d'outils repackagés (comme ERD Commander)
  - VMRC+
    - http://blogs.technet.com/keithcombs/archive/2007/06/27/vmrcplus-goes-public-download-now.aspx

Dernières vulnérabilités
Infos Microsoft (4/5)

- Mais aussi ..
  - SMS 2003 SP3
  - System Center Data Protection Manager Beta 2
  - SQL Server 2008 CTP
  - .NET 3.5 CTP
  - Codename "Acropolis" CTP
  - Nom de code "Stirling", le successeur de ForeFront
  - Note : liste des prérequis pour installer Forefront Serveur
    - .NET Framework 2.0
    - Group Policy Management Console (GPMC) SP1
    - Microsoft Management Console (MMC) 3.0
    - SQL Server 2005 SP1 (avec Database Services, Integration Services, Reporting Services, Workstation components)
    - Internet Information Services (IIS) 6.0 et ASP.NET
    - Windows Server Update Services (WSUS) 2.0 SP1

Dernières vulnérabilités
Infos Microsoft (5/5)

- Quelques sujets "polémique" (de l'anglais "troll")
  - Windows Vista, 6 mois après : plus sûr que Linux et Mac OS X ?
    - http://www.csoonline.com/pdf/6_Month_Vista_Vuln_Report.pdf
  - Apache vs. IIS
    - http://googleonlinesecurity.blogspot.com/2007/06/web-server-software-and-malware.html
  - WGA 2.0 collecte beaucoup (trop) d'information
    - http://news.softpedia.com/news/Forget-about-the-WGA-20-Windows-Vista-Features-and-Services-Harvest-User-Data-for-Microsoft-58752.shtml

Dernières vulnérabilités
Infos Vista (1/2)

- La console de récupération Vista ne demande pas de mot de passe
  - http://www.f-secure.com/weblog/archives/archive-062007.html#00001209

- "Windows Easy Transfer Companion" pour transférer ses applications sous Vista
  - http://windowsvistablog.com/blogs/windowsexperience/archive/2007/06/29/trying-out-the-windows-easy-transfer-companion-beta.aspx

Dernières vulnérabilités
Infos Vista (2/2)

- Vista Ultimate : pas beaucoup d'extras à se mettre sous la dent …
  - http://windowsultimate.com/blogs/announcements/archive/2007/07/02/update-on-the-windows-ultimate-extras.aspx
- Un portail d'information
  - http://itsvista.com/
- Comment payer ses impôts quand on est sous Vista …
  - http://www.impots.gouv.fr/portal/deploiement/p1/fichedescriptive_4187/fichedescriptive_4187.pdf

Dernières vulnérabilités
Autres avis (1/6) – failles

- *Common Vulnerability Scoring System* (CVSS) passe la seconde
  - http://www.first.org/cvss/

- Safari 3.0 (beta) pour Windows
  - 4h après sa sortie, une dizaine de failles étaient trouvées …
  - http://www.frsirt.com/bulletins/10755
  - http://www.frsirt.com/bulletins/10879

- On en a pas fini avec les failles dans les navigateurs …
  - http://lists.grok.org.uk/pipermail/full-disclosure/2007-June/063712.html

Dernières vulnérabilités
Autres avis (2/6) – failles

- TippingPoint / ZDI étiqueté "pas très éthique" par Gartner
  - Gestion de la faille QuickTime
  - http://www.scmagazine.com/us/news/article/654685/gartner-analysis-slams-tippingpoint-cansecwest-hacking-contest/

- Résultat (?) : 3Com se sépare de TippingPoint
  - http://securite.reseaux-telecoms.net/actualites/lire-3com-se-libere-de-tippingpoint-16683.html

- La relève est assurée …
  - http://www.wslabi.com/wabisabilabi/initPublishedBid.do

Dernières vulnérabilités
Autres avis (3/6) – failles Web

- Des pièges dans les liens sponsorisés
  - http://blog.washingtonpost.com/securityfix/2007/04/virus_writers_taint_google_ad.html
- Un site Google … qui n'en est pas un !
  - http://google-counter.com/
- Ca bouge dans le monde des scanners Web
  - HP rachète SPI Dynamics
  - IBM s'intéresse à WatchFire
- Plus de 10,000 sites italiens piratés en 1 week-end
  - http://www.indexel.net/1_20_4892___/Une_attaque_de_grande_envergure_contre_le_web_italien.htm

Dernières vulnérabilités
Autres avis (4/6) – failles Web

- Impact de Wikipedia sur le Web
  - Sur 600 entrées prises au hasard, 99% apparaissent dans le top 10 de Google
  - http://www.thegooglecache.com/white-hat-seo/966-of-wikipedia-pages-rank-in-googles-top-10/

- Le "Month of Search Engines Bugs" est terminé
  - 104 failles publiées
  - 44 corrigées
  - 2 remerciements

Dernières vulnérabilités
Autres avis (5/6) – malwares et spam

- Une vidéo YouTube … pour inciter à télécharger un malware !
  - http://blog.spywareguide.com/2007/07/gta_hoodlife_virus_attack_is_a.html
- Toujours de faux bulletins qui suivent le Patch Tuesday …
  - "MS07-0065"
  - http://blogs.authentium.com/virusblog/?p=178
- Des *malwares* distribués *via* la régie de publicité de Windows Live Messenger
  - http://msmvps.com/blogs/spywaresucks/archive/2007/02/18/591493.aspx
- Des virus … Symbian Signed !
  - http://www.f-secure.com/weblog/archives/archive-052007.html#00001190
- Un rootkit intéressant
  - http://www.avertlabs.com/research/blog/?p=269

Dernières vulnérabilités
Autres avis (6/6) – malwares et spam

- Les groupes antispam visés par une attaque DDoS massive
  - http://isc.sans.org/diary.html?storyid=2940
- L'Autriche (nic.at) *blacklistée* par SpamHaus
  - Le différent porte sur de nombreux sites de *phishing*
  - http://isc.sans.org/diary.html?storyid=3042
- Les campagnes en cours
  - "You have received a postcard from a family member"
    - Une campagne de recrutement de "bots" plutôt agressive
  - Le début du "spam PDF"

Dernières vulnérabilités
Autres infos (1/4)

- Une attaque très ciblée
  - http://isc.sans.org/diary.html?storyid=2853
  - Ne vise que des CEO / CFO
  - Utilise des composants packagés à l'intérieur du format RTF

- Le Pentagone victime d'intrusion via la messagerie
  - http://www.journaldunet.com/solutions/securite/actualite/07/0625-pentagone-emails-securite-informatique-us.shtml
- Le centre de Los Alamos perd des données "sensibles"
  - http://www.msnbc.msn.com/id/19418769/site/newsweek/

- Le FBI va entrer en contact avec 1 million de propriétaires de machines compromises …
  - http://www.fbi.gov/pressrel/pressrel07/botnet061307.htm

Dernières vulnérabilités
Autres infos (2/4)

- La présentation sur le "cassage" des TPM retirée de BH US 2007
  - A la demande des auteurs … et sans explication
  - http://www.networkworld.com/news/2007/062707-black-hat.html

- Le prix d'un rootkit virtualisé : $400k
  - Matasano vs. Invisible Things (Joanna Rutkowska)
  - http://securite.reseaux-telecoms.net/actualites/lire-rootkit-a-vendre-mise-a-prix-400-k$-16685.html

Dernières vulnérabilités
Autres infos (3/4)

- La France va se doter d'un portail sur la sécurité informatique
  - A destination des particuliers et des PME
  - Poussé au niveau européen par l'ENISA
  - Réalisé par la DCSSI et le CERT-A
  - En partenariat avec la CNIL, l'APRIL, Microsoft, et d'autres …

- Le SMS, reconnu comme preuve juridique dans une affaire de harcèlement
  - http://www.01net.com/article/351379.html
  - Pourtant *spoofer* l'émetteur n'est pas très compliqué …

Dernières vulnérabilités
Autres infos (4/4)

- Les processeurs Core Duo fortement bogués
  - http://www.geek.com/images/geeknews/2006Jan/core_duo_errata__2006_01_21__full.gif
  - D'après Théo de Raadt, des cas d'exploitation en mode utilisateur seraient possibles …
    - http://marc.info/?l=openbsd-misc&m=118296441702631&w=2
  - Lire aussi :
    - http://www.matasano.com/log/894/theo-de-raadt-intel-core-2-bugs-assuredly-exploitable-from-userland/
- Windows peut-il tirer partie des processeurs multi-cœurs ?
  - http://www.lemondeinformatique.fr/actualites/lire-droit-de-reponse-de-microsoft-france-23032.html

Questions / réponses

- Questions / réponses
- Date de la prochaine réunion
  - Prochaine réunion le 10 septembre 2007
- N'hésitez pas à proposer des sujets et des salles
- Bonnes vacances à tous !