OSSIR
Groupe Sécurité Windows

Réunion du 7 janvier 2008

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 (1/7)

- **Correctifs de Décembre 2007**

  - **MS07-063 Faille dans la signature SMBv2 (Q942624)**
    - **Affecte : Vista**
    - **Exploit : signature falsifiable**
    - **Crédit : n/d**

  - **MS07-064 Deux failles DirectX (Q941568)**
    - **Affecte : DirectX 7 – 10 (Vista)**
    - **Exploit :**
      - **Fichier SAMI malformé**
      - **Fichier AVI ou WAV malformé**
    - **Crédit :**
      - **Jun Mao / iDefense**
      - **Peter Winter-Smith / NGSSoftware**
      - **Jung-hyung Lee, Minseong Kim / AhnLab**

Dernières vulnérabilités
Avis Microsoft (2/7)

- MS07-065 Faille MSMQ (Q937894)
  - Affecte : Windows 2000 SP4, Windows XP SP2
  - Exploit : "buffer overflow" dans une requête RPC (?)
    - Nécessite une authentification sous Windows XP SP2
  - Crédit :
    - ZDI
    - Venustech / ADLABS

- MS07-066 Faille noyau (Q943078)
  - Affecte : Vista
  - Exploit : élévation de privilèges locale via les ALPC
  - Crédit : Thomas Garnier / SkyRecon

Dernières vulnérabilités
Avis Microsoft (3/7)

- **MS07-067 Faille dans le driver MacroVision (Q944653)**
  - **Affecte : Windows XP, Windows 2003**
  - **Exploit : élévation de privilèges locale**
  - **Crédit : n/d**

- **MS07-068 Deux failles Windows Media (Q941569, Q944275)**
  - **Affecte : Windows Media 7.1 – 11 (Vista)**
  - **Exploit : fichier ASF malformé**
  - **Crédit : Ryan Smith / X-Force**

Dernières vulnérabilités
Avis Microsoft (4/7)

- MS07-069 Quatre failles Internet Explorer (Q942615)
  - Affecte : IE toutes versions supportées (y compris IE7 / Vista)
  - Exploit : erreurs multiples
  - Crédit :
    - Peter Vreugdenhil / iDefense
    - Anonymous / ZDI
    - Sam Thomas / ZDI
    - Peter Vreugdenhil / ZDI

Dernières vulnérabilités
Avis Microsoft (5/7)

- **Prévisions pour Janvier 2008**
  - 1 bulletin critique affectant toutes les versions de Windows
  - 1 bulletin important affectant toutes les versions de Windows
- **Advisories**
  - Q942615 : problèmes de compatibilité identifiés avec MS07-069
    - Réintroduction du problème avec le filtre de décompression

Dernières vulnérabilités
Avis Microsoft (6/7)

- **Révisions**
  - **MS06-078 Faille Windows Media Player 6.4**
    - **Version 4.0 : les versions 64 bits de Windows sont également vulnérables**
  - **MS07-063 Faille dans la signature SMBv2**
    - **Version 1.1 : informations complémentaires sur la suppression du patch**
  - **MS07-064 Failles DirectX**
    - **Version 1.1 : SMS 2.0 ne supporte pas la version DirectX livrée avec Windows 2000**
    - **Version 1.2 : informations complémentaires sur la suppression du patch sous Vista**
  - **MS07-065 Faille MSMQ**
    - **Version 1.1 : authentification requise pour exploiter la faille**
    - **Version 1.2 : Windows 2000 = Pro + Server**

Dernières vulnérabilités
Avis Microsoft (7/7)

- **MS07-066 Faille noyau**
  - **Version 1.1 : faille dangereuse quels que soit les droits utilisateur**
  - **Version 1.2 : informations complémentaires sur la suppression du patch**
- **MS07-067 Faille Macrovision**
  - **Version 1.1 : précisions sur l'impact**
- **MS07-068 Failles Windows Media**
  - **Version 1.1 : informations complémentaires sur la suppression du patch sous Vista**
- **MS07-069 Failles Internet Explorer**
  - **Version 1.1 : mise en page**
  - **Version 1.2 : problème de compatibilité + informations complémentaires sur la suppression du patch sous Vista**
  - **Version 1.3 : référence à Q942615**

Dernières vulnérabilités
Infos Microsoft (1/4) - sorties

- Sorties logicielles
  - Office 2007 SP1
- Preview
  - Activation automatique des ActiveX (avril 2008)
    - http://blogs.msdn.com/ie/archive/2007/12/11/ie-automatic-component-activation-preview-now-available.aspx
  - IE 8
    - http://blogs.msdn.com/ie/archive/2007/12/19/internet-explorer-8-and-acid2-a-milestone.aspx
- La communication Microsoft
  - http://www.arcready.com/
  - http://www.wearemicrosoft.com/
  - http://www.microsoft.com/windows/products/winfamily/ie/confidence/default.mspx

Dernières vulnérabilités
Infos Microsoft (2/4) - sécurité

- La faille dans les fichiers ".mdb" commence à être exploitée
  - http://www.pcworld.com/article/id,140493-c,hackers/article.html
  - Rappel : Microsoft n'a pas l'intention de patcher
- Microsoft "achète" EP_X0FF
  - L'un des meilleurs contributeurs de rootkit.com
  - Auteur de "Rootkit Unhooker" et "Secured Eye"
  - http://www.rootkit.com/blog.php?newsid=830
- Security Vulnerability Research & Defense Blog
  - http://blogs.technet.com/swi/
- Rappel : Office 2003 SP3 bloque les formats "hérités"
  - http://www.silicon.fr/fr/news/2008/01/04/le_sp3_de_microsoft_office_bloque_certains_fichiers

Dernières vulnérabilités
Infos Microsoft (3/4) - Vista

- Vista "Biggest Tech Disappointments of 2007"
  - http://www.pcworld.com/article/id,140583-page,5-c,techindustrytrends/article.html
- Vista SP1 ne désactivera plus les copies pirates de Vista
  - http://www.engadget.com/2007/12/04/vista-sp1-kills-the-wga-kill-switch/
- Le PC le plus rapide pour faire tourner Vista est … un Mac !
  - http://www.pcworld.com/article/id,136649-page,3-c,notebooks/article.html

Dernières vulnérabilités
Infos Microsoft (4/4) - Vista

- "Notable Changes in Windows Vista Service Pack 1 Release Candidate"
  - http://technet2.microsoft.com/WindowsVista/en/library/005f921e-f706-401e-abb5-eec42ea0a03e1033.mspx?mfr=true
  - Amélioration des performances
    - Jusqu'à +50% sur la copie de fichiers
  - Amélioration du PRNG
  - API pour contrôler DEP et PatchGuard
  - Système de fichiers exFAT
  - Client VPN SSL
  - Compatibilité avec "EU Digital Signature Directive and National ID"
  - Virtualisation du KMS possible
  - Suppression de la GPMC
  - Et surtout …
    - "SP1 reduces the number of UAC (User Account Control) prompts from 4 to 1 when creating or renaming a folder at a protected location."
  - Taille du Service Pack (pour 5 langues) : 450 Mo …

Dernières vulnérabilités
Autres avis (1/7) – failles

- Faille dans un contrôle ActiveX installé par HP
  - http://www.anspi.pl/~porkythepig/hp-issue/kilokieubasy.txt
- Nombreuses failles corrigées dans Flash 9.0.115
  - http://isc.sans.org/diary.html?storyid=3765
  - Par ailleurs la méthode connect() peut désormais être restreinte
    - http://kb.adobe.com/selfservice/viewContent.do?externalId=kb402956
- 2 "0day" vendus dans la nature
  - Real Player 11 : http://gleg.net/realplayer11.html
  - Real Server : http://gleg.net/realserver.html
  - Solution : désinstaller Real Player …

Dernières vulnérabilités
Autres avis (2/7) – malwares et spam

- RealMedia : un format dangereux également
  - Fichiers .rm /.rmvb
    - http://www.avertlabs.com/research/blog/index.php/2007/12/13/be-careful-of-real-media-files-downloaded-from-the-internet/
- W32/Heiku : le retour de la disquette !
  - Folder.htt + Desktop.ini + Active Desktop
    - http://www.avertlabs.com/research/blog/index.php/2007/12/12/worm-propagation-via-floppies-revisited/
- W32/Voterai : devrait disparaître après les élections Kenyanes …
  - Le 27 décembre 2007

Dernières vulnérabilités
Autres avis (3/7) – malwares et spam

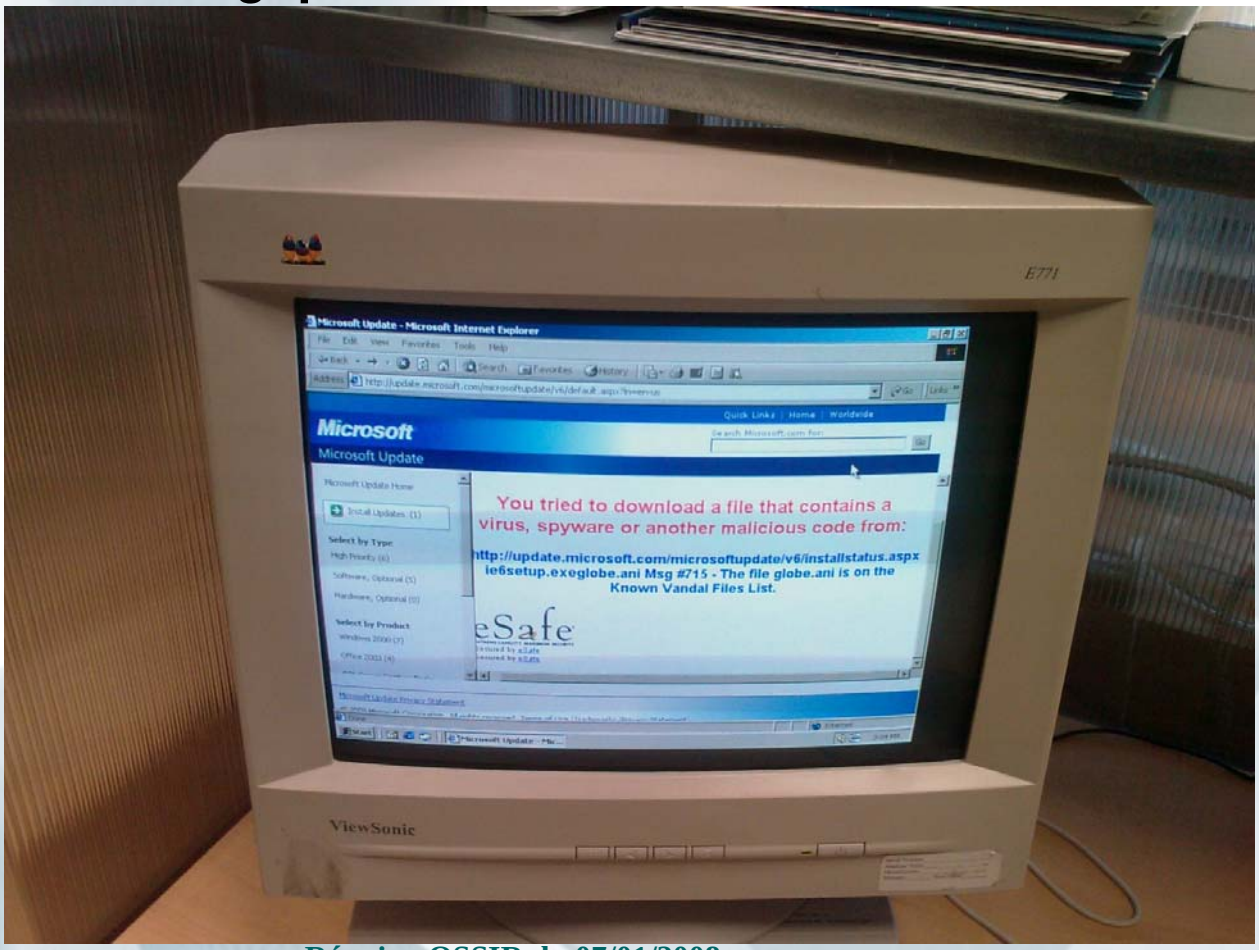
- **W32/Autorun.worm.i.gen : un virus astucieux**
  - **Utilise le nom d'un document existant et ajoute ".EXE"**
    - **http://www.avertlabs.com/research/blog/index.php/2007/12/26/morphing-your-own-documents-into-2008/**
- **Qhost.WU remplace les liens sponsorisés de Google**
  - **http://www.silicon.fr/fr/news/2007/12/20/un__trojan__exploite_les_liens_sponsorises_de_google**
- **Le blog de F-Secure défacé par des pirates turcs**
  - **Version vulnérable de Snitz Forum**
    - **http://www.f-secure.com/weblog/archives/00001336.html**

Dernières vulnérabilités
Autres avis (4/7) – attaques 2.0

- Un ver se propage sur le site Orkut
  - http://www.f-secure.com/weblog/archives/00001342.html
- Une application clairement malicieuse sur Facebook
  - http://www.tech.co.uk/computing/internet-and-broadband/news/secret-crush-virus-spreading-on-facebook?articleid=1798108733
- Encore une attaque très ciblée contre le logiciel Ichitaro au Japon
  - http://www.avertlabs.com/research/blog/index.php/2007/12/17/exploit-tarodropd-cyber-espionage-in-reality/
- Une attaque en phishing pour visiter un laboratoire américain ultra-sensible
  - http://www.silicon.fr/fr/news/2007/12/10/usa___un_laboratoire__top_secret__est_victime_de_phishers

Dernières vulnérabilités
Autres avis (5/7) – attaques 2.0

- **Faux positif ou vraie compromission ?**
  - **http://erratasec.blogspot.com/2008/01/wow.html**



Dernières vulnérabilités
Autres avis (6/7) – attaques 2.0

- Les prévisions pour 2008
  - http://www.zdnet.fr/galerie-image/0,50018840,39376953-1,00.htm

1. attaque sur les réseaux sociaux
2. attaque autour des mondes virtuels
3. Vista pris pour cible
4. évolution des bots et rootkits
5. attaques par les applications hébergées
6. attaques par VoIP
7. développement des attaques par mobile
8. utilisation du MP3 pour le spam

Dernières vulnérabilités
Autres avis (7/7) – just for fun

- Le "best of" 2007
  - http://www.lemondeinformatique.fr/actualites/lire-les-10--pertes-de-donnees--les-plus-surprenantes-de-l-annee-24802.html
- Microsoft retire son "Père Noël" en vitesse
  - http://techno.branchez-vous.com/actualite/2007/12/microsoft_retire_son_pere_noel.html
- Orange chouchoute ses clients
  - http://www.lefigaro.fr/actualites/2007/12/19/01001-20071219ARTFIG00387-lincroyable-mot-de-passe-dorange.php
- La police française bientôt autorisée à pirater ?
  - http://www.01net.com/editorial/367276/la-police-bientot-autorisee-a-installer-des-logiciels-espions-sur-les-pc/

Dernières vulnérabilités
Autres infos (1/1)

- Et pendant ce temps là sur la mailing liste de l'OSSIR

  - Droits et devoirs de l'Internet au bureau
  - Certifications en sécurité
  - Coder un générateur aléatoire
  - Compromission de SquirrelMail
  - Flash Player pour Solaris

Questions / réponses

- Questions / réponses
- Date de la prochaine réunion
  - Prochaine réunion le 11 février 2008
  - N'oubliez pas l'Assemblée Générale demain !
  - Et bonne année à tous …
- N'hésitez pas à proposer des sujets et des salles