OSSIR
Groupe Sécurité Windows

Réunion du 5 février 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 (1/4)

- **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**

Dernières vulnérabilités
Avis Microsoft (2/4)

- **Correctifs de Janvier 2007**
  - **Déjà présentés lors de la réunion du 15 janvier**
- **Correctifs prévus pour Février 2007**
  - **Information non disponible pour le moment**
- **Mises à jour "non sécurité" en janvier**
  - **.NET Framework 3.0**
  - **Client RDP 6.0**
  - **Modification du changement d'heure aux USA et dans 70 pays**

Dernières vulnérabilités
Avis Microsoft (3/4)

- **Advisories**
  - **Q932114 : encore un "0day" dans Word 2000 …**
    - **Le 4ème en 2 mois**
  - **Q932553 : et encore un "0day" dans Excel (toutes versions)**
    - **Affecte en fait toute la suite Office, mais seul Excel a été visé pour le moment**

Dernières vulnérabilités
Avis Microsoft (4/4)

- **Révisions**
  - **MS07-002**
    - **Version 2.0 : problème identifié avec Excel 2000**
  - **MS07-003**
    - **Version 1.1 : incompatibilité avec Microsoft CRM**

Dernières vulnérabilités
Infos Microsoft (1/1)

- **Sortie de Vista pour le grand public**
  - **30 janvier 2007**
  - **Bill Gates sur TF1 !**
  - **Les frères Bogdanov aux TechDays !**
- **La liste des "produits de sécurité" disponibles en même temps que Vista**
  - **http://www.microsoft.com/Presspass/press/2007/jan07/01-16SecuritySupportPR.mspx**
- **Fundamental Computer Investigation Guide For Windows**
  - **http://www.microsoft.com/technet/security/guidance/disasterrecovery/computer_investigation/default.mspx**
- **Jim Allchin quitte Microsoft**
  - **http://windowsvistablog.com/blogs/windowsvista/archive/2007/01/31/what-comes-next.aspx**

Dernières vulnérabilités
Autres avis (1/3) – failles

- **Pourquoi il faut toujours mettre à jour sa JVM …**
  - **Affecte : JVM < 1.5.10**
  - **Exploit : Exécution de code via fichier GIF malformé**
    - **http://www.zerodayinitiative.com/advisories/ZDI-07-005.html**

- **$75,000+ la faille Vista …**
  - **http://archives.neohapsis.com/archives/fulldisclosure/2007-01/0315.html**

- **La première faille "remote" dans Vista ? ☺**
  - **Entrer dans un bureau et hurler "shutdown"**
  - **http://blogs.zdnet.com/Ou/?p=416**

Dernières vulnérabilités
Autres avis (2/3) – failles (obscures)

- **Exécution de code à l'ouverture d'un fichier ".RC"**
  - **Affecte : Visual Studio 6 SP6**
  - **Exploit :**
    - **http://www.anspi.pl/~porkythepig/visualization/rc-kupiekrowe.cpp**

- **Exécution de code à l'ouverture d'un fichier ".HPJ" ou ".CNT"**
  - **Affecte : Microsoft Help Workshop**
  - **Exploit :**
    - **http://www.anspi.pl/~porkythepig/visualization/hpj-x01.cpp**
    - **http://www.anspi.pl/~porkythepig/visualization/cnt-expl1.cpp**

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

- **Les problèmes de concurrence dans les navigateurs**
  - **Affecte : toutes les versions d'IE**
  - **Exploit :**
    - **http://lcamtuf.coredump.cx/iediex/iediex.html**

- **Même les techniques de fuzzing continuent à fonctionner**
  - **Affecte : IE5 -> IE 7**
  - **Exploit :**
    - **Déni de service via une propriété malformée**
    - **http://www.determina.com/security.research/vulnerabilities/activex-bgcolor.html**
    - **<script language="JavaScript"> obj = new ActiveXObject("giffile"); obj.bgColor; </script>**

Dernières vulnérabilités
Autres avis (1/5) – virus et spywares

- **Un instituteur (américain) poursuivi pour avoir laissé un malware pornographique sur un poste scolaire**
  - **http://www.avertlabs.com/research/blog/?p=174**
- **Une idée originale**
  - **$1 pour se désinscrire d'une liste de spam**
    - **http://www.avertlabs.com/research/blog/?p=176**
  - **Probablement autorisé par la loi Russe …**
    - **http://www.russianlaw.net/english/ae06.htm**
- **Une liste des "arnaques" les plus fréquentes**
  - **http://news.bbc.co.uk/1/hi/magazine/4685868.stm**

Dernières vulnérabilités
Autres avis (2/5) – virus et spywares

- **25% de l'Internet mondial contrôlé par des bots (!)**
  - **Source : Vinton Cerf, World Economic Forum**
  - **http://news.bbc.co.uk/1/hi/business/6298641.stm**
  - **Les experts s'accordent plutôt sur 7% à 10%**
- **Le GPS TomTom GO910 infecté en usine par un virus**
  - **Le virus n'est pas actif sur l'équipement (virus PC)**
  - **http://www.tomtom.com/news/category.php?ID=2&NID=349&Language=1**
- **Une "interview" avec Corpse, l'auteur de Haxdoor**
  - **http://computersweden.idg.se/2.139/1.93344**
  - **Le journaliste se fait passer pour un client potentiel**
  - **$3,000 le logiciel + le support (serveurs, etc.)**

Dernières vulnérabilités
Autres avis (3/5) – virus et spywares

- **Un "scam 419" d'un nouveau genre**
  - **Utilisation du site de "networking" Ecademy**
  - **http://www.theregister.co.uk/2007/01/29/ecademy_419_scam/**
- **La revente d'objets WoW interdite sur eBay**
  - **http://news.cnet.co.uk/software/0,39029694,49287317,00.htm**
  - **Comment cela va-t-il affecter le monde du malware ?**
- **Virus Bulletin "VB100 Award" pour Vista32**
  - **http://www.virusbtn.com/virusbulletin/archive/2007/02/vb200702-comparative**
  - **Presque tous les antivirus l'obtiennent ...**
    - **… sauf Microsoft OneCare !**

Dernières vulnérabilités
Autres avis (4/5) – virus et spywares

- **Vrai ou faux ?**

citibank

New sign on procedure for all users

Why will Citibank Online be even more secure?

Dear [illegible],

When banking online, your security is Citibank's number one priority. To offer you even greater protection, Citibank Online is introducing a new sign on procedure that will be even more secure, but easier for you to remember.

You set the combination yourself

Your current card number and ATM PIN sign on will be replaced with:

* A new User ID and Password, both of which you create yourself
* PLUS three important "Security Questions" you choose yourself

Because you create your own sign on details, it's easier to remember your combination - but much more difficult for anyone else to figure out. Plus, we've enhanced our site navigation to make your online banking experience even easier.

These changes will take place over the next few months. The chart explains the simple steps you'll be guided through to set up your new sign on. For updates on the launch of the new Citibank Online website, check www.citibank.com.au.

Go to www.citibank.com.au and click "Sign on to Citibank Online"

STEP 1	When the new sign on process is introduced you will notice a new button called "**First time here? Create your User ID**". Please select this option.
STEP 2	To identify and authenticate yourself, enter: **(a)** Your card number (Citicard or credit card) **(b)** Your ATM PIN **(c)** Your account number (For Citibank Credit Card customers this is your credit card number), then click the "**Continue**" button.
STEP 3	You will be guided to create your own **User ID, Password** and three "**Security Questions**". You will be asked to choose from a range of questions. Each time you sign on you will be asked one question.

Dernières vulnérabilités
Autres avis (5/5) – virus et spywares

- **Une épidémie de malware "à l'ancienne" (Small.DAM)**
  - **Un titre accrocheur**
    - **Russian missle shot down USA satellite**
    - **Chinese missile shot down USA aircraft**
    - **Sadam Hussein alive!**
    - **Radical Muslim drinking enemies' blood.**
  - **Une pièce jointe exécutable**
    - **Full Clip.exe, Full Story.exe, Read More.exe, Video.exe , …**
    - **Génération rapide de variantes multiples**
  - **Une épidémie**
    - **http://www.youtube.com/watch?v=kH8cS1AkqiI**
  - **Un réseau de contrôle P2P sur le port UDP/4000**

Dernières vulnérabilités
Autres avis (1/1)

- **La réponse de Microsoft à Peter Gutmann**
  - **http://windowsvistablog.com/blogs/windowsvista/archive/2007/01/20/windows-vista-content-protection-twenty-questions-and-answers.aspx**
- **Un "pirate" arrêté en France pour "possession d'outils de sécurité sans motif légitime"**
  - **http://www.01net.com/editorial/338943/securite/un-pirate-interpelle-a-marseille/**
- **175,000 clés USB distribuées aux étudiants en Ile-de-France**
  - **Pré-équipées avec les versions "portables" des logiciels libres les plus connus (FireFox, Thunderbird, …)**
  - **Mais en version Windows ☺**

Questions / réponses

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