OSSIR
Groupe Sécurité Windows

Réunion du 2 avril 2007

Revue des dernières vulnérabilités Microsoft

Cette veille est réalisée par les coanimateurs du groupe Windows

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

EdelWeb

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 Mars 2007**
  - **Aucun !**
  - **A part Windows 2003 SP2 …**
    - **Aucun correctif de sécurité d'après Microsoft**
    - **Ou pas …**
      - **http://isc.sans.org/diary.html?storyid=2454**
- **Correctifs de Avril 2007**
  - **Prévu pour le 3 avril**
  - **1 bulletin critique pour Windows**
    - **Faille ANI**

Dernières vulnérabilités
Avis Microsoft (3/5)

- **Advisories**

  - **Q935423 - faille dans le traitement des curseurs animés ".ANI"**
    - **Affecte "user32.dll" dans Windows 2000, XP SP2, 2003, Vista**
    - **"0 day" en cours d'exploitation**
      - **Via un fichier ANI, une page web ou un email**
      - **Indépendant de l'extension**
      - **Un ver en provenance de Chine se propage déjà**
        - **http://www.cisrt.org/enblog/read.php?68**
    - **Position de Microsoft**
      - **Au courant de la faille depuis le 20 décembre 2006**
        - **Date de la découverte par Alexander Sotirov (Determina)**

Dernières vulnérabilités
Avis Microsoft (4/5)

- **Solutions**
  - **Signature antivirus**
  - **Patch non officiel**
    - **http://research.eeye.com/html/alerts/zeroday/20070328.html**

- **Quelques analyses**
  - **http://asert.arbornetworks.com/2007/03/any-ani-file-could-infect-you/**
  - **http://isc.sans.org/diary.html?storyid=2534**
  - **http://isc.sans.org/diary.html?storyid=2539**
  - **http://www.mnin.org/write/ani-notes.pdf**

Dernières vulnérabilités
Avis Microsoft (5/5)

- **Révisions**
  - **MS06-042**
    - **Version 3.2 : problème détecté sur XP SP2 avec IE 6**
  - **MS06-077**
    - **Version 1.1 : clé de type REG_SZ et non REG_DWORD ☺**

Dernières vulnérabilités
Infos Microsoft (1/2)

- **"Malware Revolution: A Change in Target"**
  - **http://www.microsoft.com/technet/community/columns/secmgmt/sm0307.mspx**
- **MSXML 4 sera désactivé dans IE par "Kill Bit" d'ici la fin de l'année**
  - **http://blogs.msdn.com/xmlteam/archive/2007/03/12/msxml4-is-going-to-be-kill-bit-ed.aspx**
- **MSUS arrive en fin de vie**
  - **Prévu pour le 10 juillet 2007**
- **Vista se vend 2 fois plus vite que Windows XP**
  - **20 million de copies écoulées en 1 mois**
    - **http://www.referencement-internet-web.com/20070327-Microsoft-vend-Vista-Windows-XP.php**
  - **Mais ceci inclut les gens ayant un bon d'échange XP -> Vista !**
- **Vista contre Vista**
  - **http://www.senioractu.com/Vista-une-chaine-senior-avec-Philippe-Gildas-prevue-pour-la-rentree-2007_a7028.html**

Dernières vulnérabilités
Infos Microsoft (2/2)

- **Si vous devez piratez quelque chose … piratez Windows !**
  - **http://www.theregister.co.uk/2007/03/13/ms_piracy_benefits/**

- **Ca tombe bien, c'est déjà fait**
  - **Activation OEM par patch du BIOS**
    - **http://fr.news.yahoo.com/05032007/308/piratage-un-crack-pour-vista-parfaitement-fonctionnel.html**
    - **Auteur : Paradox ☺**
  - **Clé SkipRearm**
    - **http://www.windowssecrets.com/comp/070315/**
  - **Keygen par bruteforce**
    - **http://keznews.com/2431_Vista_Brute_Force_Keygen**
    - **En fait celui là serait un *hoax* ☺**

- **Client TSE v6 disponible**
  - **Amélioration visuelle : multi-écrans, 32 bits, lissage des polices**
  - **Support RDP over HTTPS via serveur passerelle**
  - **Nouveau mécanisme d'authentification : NLA et serveur**
  - **http://support.microsoft.com/kb/925876**

Dernières vulnérabilités
Autres avis (1/10) – failles

- **"Faille" DDNS**
  - **Affecte : toutes versions de Windows**
  - **Exploit : combinaison de 2 attaques**
    - **Enregistrement d'un nouveau nom**
      - **Possible via WINS, création de compte machine, DNS Dynamique non sécurisé …**
    - **Utilisation du nom réservé "WPAD" pour rediriger les accès Internet**
      - **WPAD = Windows Proxy AutoDiscovery**

- **Déni de service local via le pilote "ndistapi.sys"**
  - **Affecte : Windows XP SP2, Windows 2003 SP0/SP1**
  - **Exploit : écriture de données malformées dans "\Device\NdisTapi"**
    - **http://www.reversemode.com/index.php?option=com_remository&Itemid=2&func=fileinfo&id=47**

Dernières vulnérabilités
Autres avis (2/10) – failles

- **"Faille" Windows Mail**
  - **Affecte : Windows Vista**
  - **Exploit : si un programme et un répertoire possèdent le même nom, alors il est possible d'exécuter le programme via un lien "file://"**
    - **Très limité en pratique**
      - **Seul 2 programmes affectés : migwiz.exe et winrm.cmd**
      - **Impossible de passer des paramètres**
    - **"http://hostile.com/malware.exe" semble plus efficace ☺**
    - **Vecteur intéressant (à l'intérieur d'une entreprise) : les chemins UNC**

Dernières vulnérabilités
Autres avis (3/10) – failles

- **Une nouvelle faille dans QuickTime**
  - **Le "HREF Tracker" permet d'ouvrir automatiquement un contenu actif lié**
  - **Déjà exploité sur MySpace …**
    - **http://didierstevens.wordpress.com/2007/03/12/p0wned-by-a-qt-movie/**
  - **Note : JavaScript est totalement désactivé à partir de QuickTime 7.1.5**
    - **http://developer.apple.com/documentation/QuickTime/Conceptual/QTScripting_JavaScript/bQTScripting_JavaScri_Document/chapter_1000_section_4.html**

Dernières vulnérabilités
Autres avis (4/10) – failles Web

- **Le portail Windows Live italien "empoisonné" par de faux sites**
  - **http://sunbeltblog.blogspot.com/2007/03/malware-authors-take-over-live-searches.html**
  - **Problème récurrent dans les moteurs de recherche**
    - **Cf. présentation de Laurent Oudot, Hack.lu**

- **Spoofing d'adresse via la propriété "onUnload"**
  - **Affecte : nombreux navigateurs dont IE 6 / IE 7**
  - **Exploit : http://lcamtuf.coredump.cx/ietrap/**

- **Contournement des filtres anti-XSS via un codage UTF-7**
  - **Affecte: nombreux navigateurs dont IE7**
  - **Exploit : http://www.hardened-php.net/advisory_032007.142.html**

Dernières vulnérabilités
Autres avis (5/10) – virus et spywares

- **Vbootkit**
  - **Un rootkit de boot "compatible Vista"**
  - **http://www.rootkit.com/newsread.php?newsid=671**
- **Kaspersky vs. Vista**
  - **"Une fois UAC désactivé, Vista est moins sûr que XP"**
  - **http://news.zdnet.co.uk/security/0,1000000189,39286362,00.htm**
- **Le spam … tue !**
  - **http://www.theregister.co.uk/2007/03/23/net_pills_poison_woman/**

Dernières vulnérabilités
Autres avis (6/10) – virus et spywares

- **Symantec fait beaucoup de bruit …**
  - **Symantec vs. Vista**
    - **De bon papiers de recherche**
      - **http://www.symantec.com/enterprise/theme.jsp?themeid=vista_research**
    - **Ex. "58% des malwares existant sont compatibles Vista"**
  - **"Vista est le plus sûr des OS"**
    - **http://www.internetnews.com/security/article.php/3667201**
  - **John Thompson (CEO Symantec) :**
    - **"It's a huge conflict of interest for one company to provide both an operating platform and a security platform"**
      - **http://www2.csoonline.com/blog_view.html?CID=32554**
  - **Bilan de l'année 2006 vue par Symantec**
    - **http://www.symantec.com/about/news/release/article.jsp?prid=20070319_01**

Dernières vulnérabilités
Autres avis (7/10) – virus et spywares

- **Un lecteur de cartes mémoires Epson infecté par un virus**
  - **http://www.erenumerique.fr/epson_p_2500_virus_inside-news-9058.html**
- **Le nombre de machines infectées par des bots a triplé en mars**
  - **http://www.shadowserver.org/wiki/pmwiki.php?n=Stats.BotCounts**
- **Un malware ciblé attaque une banque norvégienne**
  - **Quelques innovations techniques**
    - **Coupe le son pour rendre les popups moins agressives ☺**
  - **http://www.websense.com/securitylabs/blog/blog.php?BlogID=113**
- **Un autre malware original**
  - **"Iframe-Cash" alias "Iframe-Dollars"**
    - **Injecte du code HTML dans la page Web originale**
    - **Configurable par un fichier XML**
    - **Qualité "professionnelle"**

Dernières vulnérabilités
Autres avis (8/10) – virus et spywares

- **Opération "Spamalot"**
  - **La SEC (équivalent de la COB) suspend les cotations des entreprises visées par du spam de manipulation de cours**
  - **Problèmes :**
    - **La réactivité**
    - **La durée de suspension**
    - **Les effets de bord**
  - **http://www.avertlabs.com/research/blog/?p=217**

- **Microsoft OneCare n'obtient que 82% à la détection "in the wild"**
  - **http://www.av-comparatives.org/**

- **Trend Micro "rachète" HijackThis!**
  - **http://www.reseaux-telecoms.net/actualites/lire-trend-micro-rachete-un-editeur-d-antispyware-gratuit-15762.html**

- **Symantec achète 4FrontSecurity**
  - **http://solutions.journaldunet.com/breve/securite/10016/symantec-rachete-4frontsecurity-acteur-de-la-gestion-de-risque.shtml**

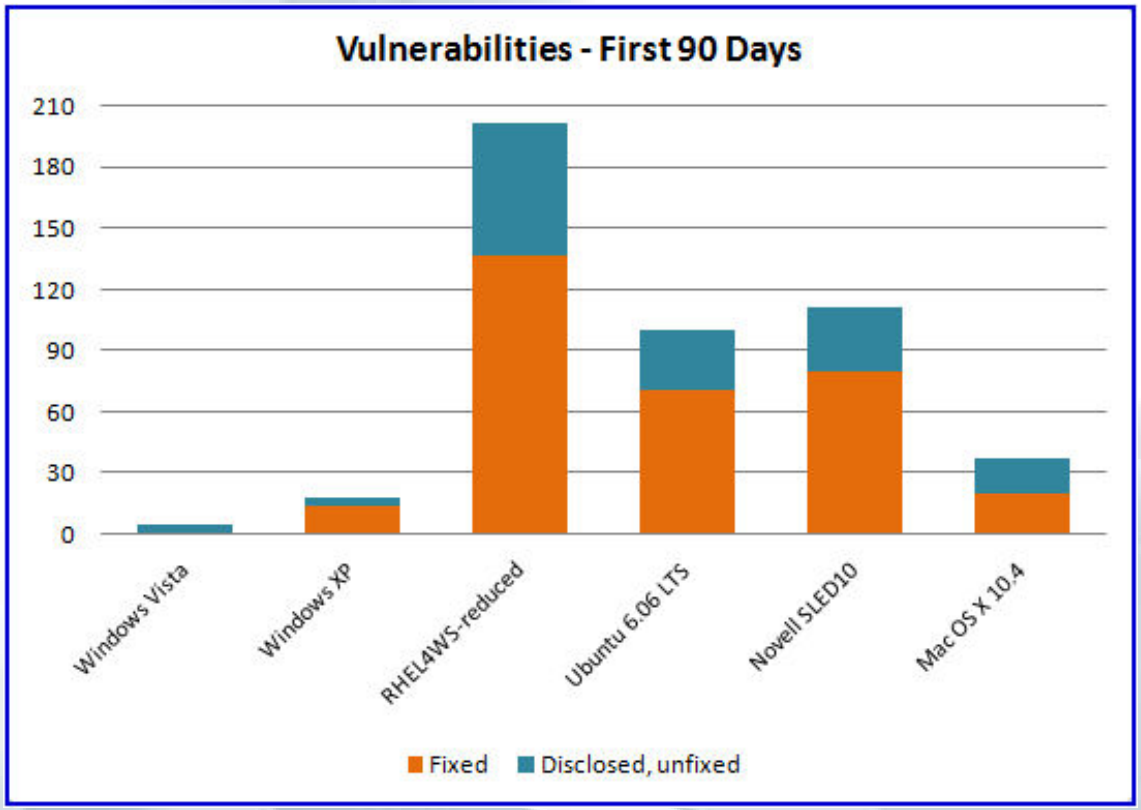
Dernières vulnérabilités
Autres avis (9/10) – virus et spywares

- **Vulnérabilité dans Trend Micro et Kaspersky**
  - **Déni de service via un fichier UPX malformé**
  - **http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=485**
  - **http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=488**

- **Nouvelles solutions**
  - **McAfee VirusScan v8.5i**
    - **Fonctionnalités anti-rootkit**
  - **Kaspersky Anti-virus Mobile**
    - **Contrôle des fichiers synchronisés mais aussi SMS / MMS**

Dernières vulnérabilités
Autres avis (10/10) – virus et spywares

- **Comparatif des vulnérabilités par système, 90 jours après leur sortie**
  - **Source : Jeff Jones Security Blog (employé Microsoft)**
    - **http://blogs.technet.com/security**



Dernières vulnérabilités
Autres infos (1/3)

- **Metasploit 3.0 est sorti**

- **The Week of Vista Bugs**
  - **https://www.securinfos.info/english/the-week-of-vista-bugs.php**

- **45 million de numéros de CB volés**
  - **http://news.bbc.co.uk/1/hi/business/6508983.stm**
  - **Les pirates étaient dans le réseau de "TK Maxx" depuis 1 an et demi …**

- **Un projet d'attentat contre Internet déjoué en Angleterre ?**
  - **http://www.timesonline.co.uk/tol/news/uk/crime/article1496831.ece**
  - **Un plan simple : faire sauter l'immeuble de Telehouse …**

Dernières vulnérabilités
Autres infos (2/3)

- **L'ENISA publie "Towards future Risk scenarios in Europe"**
  - **http://www.enisa.europa.eu/pages/02_01_press_2007_03_19_ENISA_Study_Emerging_Risks.html**
  - **3 risques pour 2010**
    - **Attaque sur les mobiles**
    - **Collection et agrégation de données personnelles**
    - **Interdépendance des infrastructures du monde "réel"et d'Internet**

- **La coalition anti-spyware publie un guide de "bonnes pratiques"**
  - **http://www.antispywarecoalition.org/documents/**

Dernières vulnérabilités
Autres infos (3/3)

- **Et pendant ce temps là sur la mailing liste de l'OSSIR**
  - **Liste SUR**
    - **Dans la série "Month of Bugs"...**
    - **X509 - PKI : Retour d'expérience sur un déploiement proche militaire ?**
    - **Streaming via video flash sans copie locale**
  - **Liste NT**
    - **Toujours à propos de sécurité Vista**
    - **Microsoft Windows 0-day ANI vulnerability (CVE-2007-0038)**

Questions / réponses

- **Questions / réponses**
- **Date de la prochaine réunion**
  - **Conférence JSSI le 22 mai 2007**
  - **Prochaine réunion le 11 juin 2007**
- **N'hésitez pas à proposer des sujets et des salles**