OSSIR
Groupe Sécurité Windows

Réunion du 12 mars 2007

Revue des dernières vulnérabilités Microsoft

Cette veille est réalisée par les coanimateurs du groupe Windows

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

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

EdelWeb

Dernières vulnérabilités
Avis Microsoft (1/10)

- **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 (2/10)

- **Correctifs de Février 2007**

Bulletin	Faille	Affecte	Détails	Exploit
MS07-005	**Vulnérabilité dans Step-by-Step Interactive Training** (Brett Moore)	**Microsoft Interactive Training 3.x (XP, 2000, 2003)**	**Buffer overflow dans les fichiers bookmark .cbo .cbl .cbm →Exécution de code**	**Non**
MS07-006	**Vulnérabilité dans Windows Shell** (nc)	**Windows XP, 2003**	**Service « Shell Hardware Detection » →Elévation de privilège SYSTEM**	**Non**

Dernières vulnérabilités
Avis Microsoft (3/10)

Bulletin	Faille	Affecte	Détails	Exploit
MS07-007	**Vulnérabilité dans Windows Image Acquisition** (nc)	**Windows XP**	**Service « Windows Image Acquisition » →Elévation de privilège**	**Oui (payant)**
MS07-008	**Vulnérabilité dans l'ActiveX HTML Help** (HD Moore)	**Windows 2000, XP, 2003**	**Buffer Overflow dans l'ActiveX « Hhctrl.ocx » →Exécution de code**	**Non (à venir ?)**
MS07-009	**Vulnérabilité dans un Active X MDAC** (FrSIRT!)	**MDAC 2.5, 2.6, 2.7, 2.8 (sauf SP2)**	**ActiveX ADODB.connection via méthode Execute() →Exécution de code**	**PoC en octobre**

Dernières vulnérabilités
Avis Microsoft (4/10)

Bulletin	Faille	Affecte	Détails	Exploit
MS07-010	**Vulnérabilité dans Microsoft Malware Protection Engine** (Neel Mehta et Alex Wheeler / ISS)	**- Windows Live OneCare - Antigen - Windows Defender - Forefront Security**	**Buffer overflow dans le contrôle des PDF →Exécution de code SYSTEM**	**Non**
MS07-011	**Vulnérabilité dans le composant OLE Dialog** (Kostya Kortchinsky / Immunity et Fabrice Desclaux / EADS-IW)	**Windows 2000, XP, 2003**	**Application qui utilise OLE Dialog pour lire un objet OLE dans un RTF →Exécution de code**	**PoC**
MS07-012	**Vulnérabilité dans le composant MFC** (Kostya Kortchinsky / Immunity et Fabrice Desclaux / EADS-IW)	**Windows 2000, XP, 2003 Visual Studio .NET 2000 / 2003**	**Application qui utilise MFC pour lire un objet OLE dans un RTF →Exécution de code**	**Non**

Dernières vulnérabilités
Avis Microsoft (5/10)

Bulletin	Faille	Affecte	Détails	Exploit
MS07-013	**Vulnérabilité dans le composant RichEdit** (Kostya Kortchinsky / Immunity et Fabrice Desclaux / EADS-IW)	Windows 200, XP, 2003 Office 2000, XP, 2003 Office 2004 Mac Learning Essentials	Application qui utilise RichEdit pour lire un objet OLE dans un RTF →Exécution de code	Non
MS07-014	**Vulnérabilité dans Word** (Weng Shih-hao / ICSTC, USAA, Andreas Marx / AV-Test)	Office 2000, XP, 2003 Works 2004, 2005, 2006 Office 2004 Mac	6 vulnérabilités exploitables en ouvrant un fichier « .doc » malformé →Exécution de code	0day depuis décembre
MS07-015	**Vulnérabilité dans Office** (Chris Ries / VigilantMinds Inc.)	Office 2000, XP, 2003 (sauf PowerPoint Viewer) Office 2004 Mac Project 2000, 2002 Visio 2002	2 vulnérabilités exploitables en ouvrant un fichier « .xls » et « .ppt » malformés →Exécution de code	0day depuis février

Dernières vulnérabilités
Avis Microsoft (6/10)

Bulletin	Faille	Affecte	Détails	Exploit
MS07-016	**Patch cumulatif pour IE** (HD Moore, iDefense)	**IE 5, 6, 7 (sauf Vista)**	**3 vulnérabilités dans les objets COM (Imjpcksid.dll, Imjpskdic.dll, Msb1fren.dll, Htmlmm.ocx, Blnmgrps.dll) et dans le client FTP « WinINet.DLL » →Exécution de code**	**Oui pour FTP (pas XP SP2)**

- **Une bonne analyse des patches Microsoft**
  - **http://isc.sans.org/diary.html?storyid=2232**

Dernières vulnérabilités
Avis Microsoft (7/10) - Synthèse

VECTEUR D'EXPLOITATION PREMIER

IMPACT MS	Internet	LAN	Utilisateur
Exécution de code à distance			**Step-by-Step IT (005)** **HTML Help (008)** **MDAC (009)** **Malware (010)** **OLE / Office (011)** **MFC / Visual Studio (012)** **Office RichEdit (013)** **Office Word (014)** **Office Excel PPT (015)** **IE (016)**
Élévation de privilèges			**Shell (006)** **Image Acquisition (007)**
Usurpation de contenu			
Déni de service			
Divulgation d'informations			

Dernières vulnérabilités
Avis Microsoft (8/10)

- **Pas de bulletins en mars**
  - **Hypothèse du SANS : la mise à jour avancée de l'heure d'été (DST) au second week-end de mars, soit le week-end qui précède la sortie des patches…**
  - **… et certains utilisateurs ont rencontré des problèmes avec le patch 931836**
    - **http://isc.sans.org/diary.html**
- **The missing Microsoft patches**
  - **http://isc.sans.org/diary.html?storyid=1940**

Dernières vulnérabilités
Avis Microsoft (9/10)

- **Advisories**
  - **Failles corrigées :**
    - **Q929433 (Word – MS07-014)**
    - **Q932114 (Word – MS07-014)**
    - **Q932553 (Office – MS07-015)**
  - **Failles "post mardi" :**
    - **Q933052 "0day" dans Word**

Dernières vulnérabilités
Avis Microsoft (10/10)

- **Révisions**
  - **MS06-058 (v1.1 – patch inefficace, utiliser MS07-015 à la place)**
  - **MS06-078 (v2.2 – problème avec la version coréenne)**
  - **MS07-002 (v2.0 – problème dans la lecture de fichiers)**
  - **MS07-006 (v1.1)**
  - **MS07-010 (v1.1)**
  - **MS07-011 (v1.1)**
  - **MS07-012 (v1.1)**
  - **MS07-013 (v1.1, v1.2)**
  - **MS07-015 (v1.1)**
  - **MS07-016 (v1.1)**

Dernières vulnérabilités
Infos Microsoft (1/3)

- **5 ans de support pour Vista (au lieu de 10)**
  - **http://support.microsoft.com/lifecycle/?p1=11712**
- **Le premier bug Vista corrigé officiellement**
  - **http://www.guwiv.com/portal/blogs/news/archive/2007/03/01/premier-correctif-pour-vista-probl-me-de-client-dns.aspx**
- **D'autres sont à venir …**
  - **http://research.eeye.com/html/advisories/upcoming/20070119a.html**
- **100 raisons de passer à Vista**
  - **http://www.microsoft.com/france/windows/products/windowsvista/100reasons.mspx**

Dernières vulnérabilités
Infos Microsoft (2/3)

- **Vista et Office 2007 vendus en téléchargement**
  - **Une première pour Microsoft !**
  - **http://www.windowsmarketplace.com/content.aspx?ctId=394&tabid=1**
- **Mark Russinovitch**
  - **"UAC n'est pas une fonction de sécurité"**
    - **http://blogs.technet.com/markrussinovich/archive/2007/02/12/638372.aspx**
  - **Commentaire :**
    - **http://theinvisiblethings.blogspot.com/2007/02/vista-security-model-big-joke.html**
- **La mise à jour "heure d'été" DST ne sera facturée que $4,000 pour les propriétaires de Windows 2000 et Exchange 2000**

Dernières vulnérabilités
Infos Microsoft (3/3)

- **Les mises à jour de sécurité sont disponibles sur des fichiers images de CD ISO-9660 sur le Centre de téléchargement Microsoft**
  - **http://support.microsoft.com/kb/913086**

- **Sorties notables**
  - **NetMon 3.0**
  - **Outils Vista**
    - **PowerShell 1.0 pour Vista**
    - **Windows AIK (Automated Installation Kit) 1.0**
    - **KMS (Key Management Service)**
    - **VAMT (Volume Activation Management Tool)**
  - **Applications "certifiées Vista" et "compatibles Vista"**
    - **http://support.microsoft.com/kb/933305**

- **Les groupes utilisateur français sponsorisés par Microsoft**
  - **http://www.shareclubs.org/**

Dernières vulnérabilités
Autres avis (1/10) – failles

- **Java 1.5.0 Update 11**
  - **La dernière mise à jour avait moins d'un mois !**
- **Encore un faille Word 2000 !**
  - **Un simple déni de service ?**
  - **http://www.avertlabs.com/research/blog/?p=199**
- **Déni de service dans la Libc de Visual Studio 2005**
  - **Toute manipulation de date > 1er janvier 3000 lève un assert()**
  - **http://securityvulns.com/advisories/year3000.asp**

Dernières vulnérabilités
Autres avis (2/10) – failles

- **Faille(s) dans Windows Mobile**
  - **Affecte : Windows Mobile 2003, 2003SE, 5.0**
  - **Exploit :**
    - **Déni de service via Internet Explorer**
    - **Déni de service via un JPEG malformé**
  - **Crédit : Trend Micro**
    - **http://blog.trendmicro.com/trend-micro-finds-more-windows-mobile-flaws/**
  - **Pas de patch disponible**
    - **Mais le déploiement serait problématique de toute façon …**

Dernières vulnérabilités
Autres avis (3/10) – failles Web

- **Contourner la "same origin policy" avec AJAX + IE**
  - **Affecte : IE**
  - **Exploit :**
    - **xmlhttp.open("GET\thttp://hostile.com/\tHTTP/1.0\n\n", "x",true);**
    - **http://lcamtuf.coredump.cx/iexmltest.html**

- **Contourner la "same origin policy" avec Flash 9 et une corruption de cache DNS ("anti-DNS pinning")**
  - **http://www.jumperz.net/index.php?i=2&a=3&b=3**

- **Accéder à file:// à l'aide du "popup blocker"**
  - **Affecte : Firefox 1.5 (au moins)**
  - **Exploit :**
    - **Combinaison de problèmes multiples**
    - **Ex. nom de fichier temporaire prédictible (utilisation de rand())**
    - **http://www.securiteam.com/securitynews/5JP051FKKE.html**

Dernières vulnérabilités
Autres avis (4/10) – failles

- **Bugs(s) critique(s) dans Firefox**
  - **Bug #1 manipulation des cookies via 'location.hostname'**
    - **Affecte : Firefox <= 2.0.0.1**
    - **Exploit :**
      - **http://lcamtuf.dione.cc/ffhostname.html**
  - **Bug #2 les scripts exécutés dans about:blank peuvent accéder à n'importe quel domaine**
    - **Affecte : Firefox <= 2.0.0.1 & IE 7 (partiellement)**
    - **Exploit :**
      - **http://lcamtuf.coredump.cx/ffblank/**
  - **Crédit : Michal Zalewski**

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

- **La guerre des gangs !**
  - **StormWorm attaque Warezov**
  - **http://www.secureworks.com/research/threats/view.html?threat=storm-worm**
  - **http://www.websense.com/securitylabs/blog/blog.php?BlogID=107**

- **La société Agoga.com achète le Cameroun !**
  - **Gestionnaire du TLD ".cm"**
  - **A mis en place un *wildcard* DNS sur le TLD**
  - **A une lettre près …**
    - **Google.cm, paypal.cm, …**

- **Plus c'est gros …**
  - **Un message ciblé envoyé à des clients de gros ISPs**
    - **"Merci de bien vouloir installer le script de sécurité ci-joint à la racine de votre serveur Web"**
  - **http://isc.sans.org/diary.html?storyid=2208**

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

- **Un virus intéressant**
  - **La deuxième partie est un ZIP chiffré avec un mot de passe construit dynamiquement**
    - **http://isc.sans.org/diary.html?storyid=2223**
- **Un auteur de virus arrêté en Chine**
  - **Suffisamment rare pour être signalé**
  - **http://news.xinhuanet.com/legal/2007-02/12/content_5731540.htm**
- **La fin du spam ?**
  - **Le Viagra en vente libre en Angleterre ☺**
  - **http://news.bbc.co.uk/1/hi/health/6351171.stm**
- **Le "Drive-By Pharming"**
  - **Javascript côté LAN + login "admin/admin" sur les routeurs ADSL**
  - **http://www.symantec.com/avcenter/reference/Driveby_Pharming.pdf**

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

- **Statistique fournie par McAfee**
  - **http://www.avertlabs.com/research/blog/?p=196**

Patch	Malware	Patch Availability	Worm Attack	Number of days for worm to appear
MS01-020	Nimda	Oct 17th, 2000	Sept18th, 2001	335 Days
MS02-061	Slammer	July 24th, 2002	Jan 25th, 2003	185 Days
MS03-026	Blaster	July 16th, 2003	Aug 11th, 2003	26 Days
MS04-011	Sasser	Apr 13th, 2004	Apr 30th, 2004	17 Days
MS05-039	Zotob	Aug 09th, 2005	Aug 14th, 2005	5 Days
MS06-040	Mocbot	Aug 08th, 2006	Aug 12th 2006	4 Days

Dernières vulnérabilités
Autres avis (8/10)

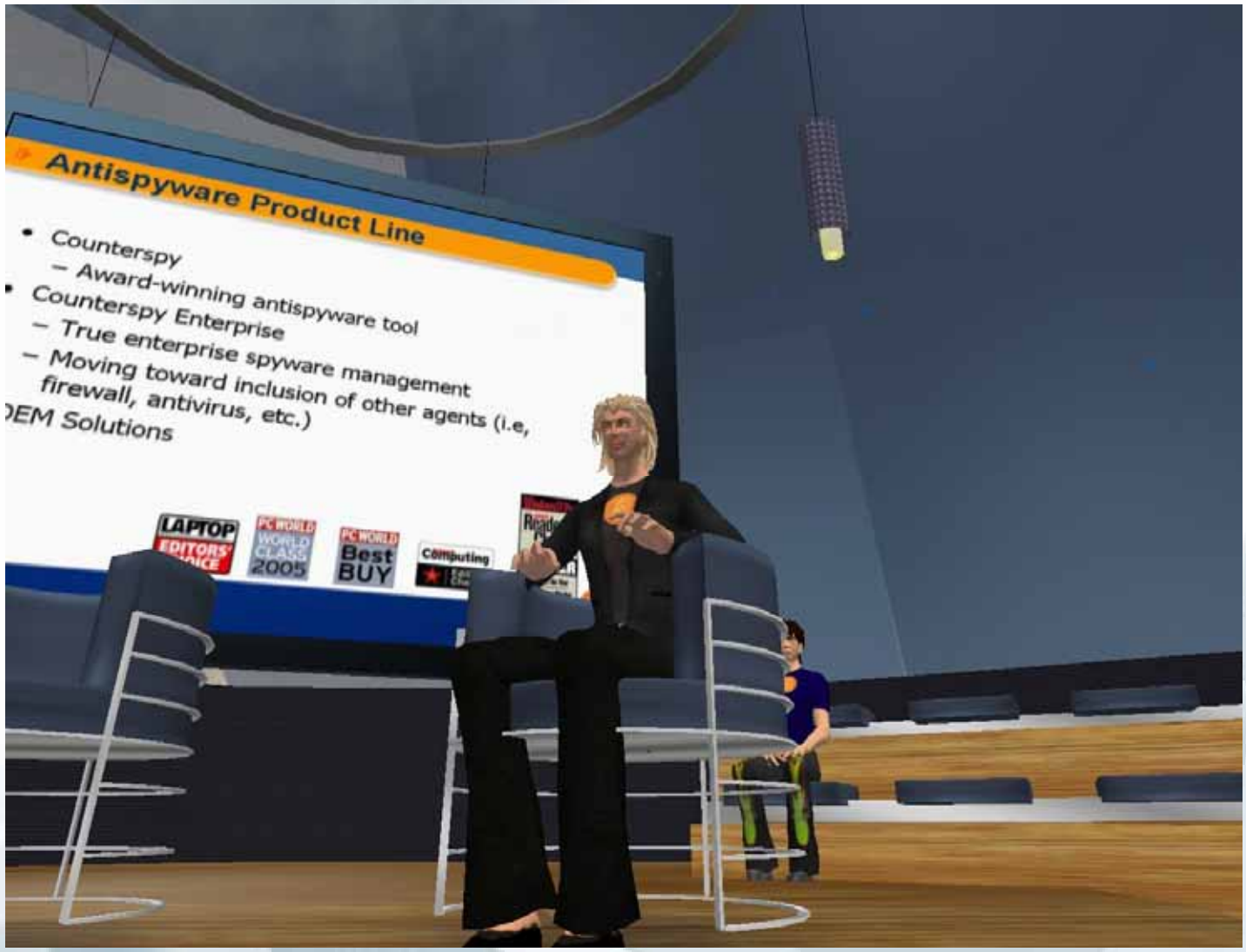
- **Le CEO de Symantec n'utilisera pas Vista**
  - **http://news.com.com/Symantec+CEO+says+no+Vista+for+me/2008-1009_3-6158821.html**
- **Réactivation du projet ElseNot**
  - **http://elsenot.com/**
- **Month of PHP Bugs en mars 2007 …**
  - **Par Stefan Esser (Hardened PHP Project)**
  - **http://www.securityfocus.com/columnists/432/3**
- **La police allemande aimerait bien instaurer la "perquisition numérique"**
  - **http://www.theregister.co.uk/2007/02/27/german_state_hackers/**

Dernières vulnérabilités
Autres avis (9/10)

- **Sortie de BackTrack 2.0**
  - **http://www.remote-exploit.org/backtrack.html**

- **La fin de l'OSSIR ? ;)**
  - **SunBelt Software organise une présentation de ses produits … dans Second Life !**
    - **http://sunbeltblog.blogspot.com/2007/02/sunbelt-software-holding-press.html**
  - ***(Merci à Tyop² pour l'info et les screenshots)***

Dernières vulnérabilités
Autres avis (10/10)



Dernières vulnérabilités
Autres infos (1/1)

- **Et pendant ce temps là sur la mailing liste de l'OSSIR**
  - **Liste SUR**
    - **Solaris, le système en bois**
    - **Sécurisation des échanges web**
    - **Tableau comparatif de fonctionnalités sécurité entre OS**
    - **De la fragilité de certains logiciels libres**
    - **Retours d'expérience LDAP et UNIX / LINUX**
  - **Liste NT**
    - **Contrôle des mouvements de fichiers**
    - **LastVersionChecker**

Questions / réponses

- **Questions / réponses**
- **Date de la prochaine réunion**
  - **Prochaine réunion le 2 avril 2007**
- **N'hésitez pas à proposer des sujets et des salles**