OSSIR
Groupe Sécurité Windows

Réunion du 11 février 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 (1/4)

- **Correctifs de Janvier 2008**

  - **MS08-001 Failles dans la pile TCP/IP**
    - **Affecte : Windows (toutes versions supportées)**
    - **Exploit :**
      - **CVE-2007-0066 : ICMP "Router Advertisement"**
        - **IPv6 non activé par défaut avant Vista**
        - **Vista non vulnérable**
      - **CVE-2007-0069 : IGMPv3 et MLDv2 (précisément "Source Specific Multicast")**
        - **XP et Vista vulnérables en configuration par défaut ! (UPnP activé)**
    - **Crédit : Alex Wheeler & Ryan Smith / IBM ISS X-Force**
      - **http://blogs.iss.net/archive/MS08-001.html**
      - **http://blogs.iss.net/archive/howtoprotectMS08-001.html**

Dernières vulnérabilités
Avis Microsoft (2/4)

- Analyses
  - http://www.zynamics.com/files/ms08001.swf
  - http://blogs.technet.com/swi/archive/2008/01/08/ms08-001-the-case-of-the-moderate-important-and-critical-network-vulnerabilities.aspx
- Code d'exploitation
  - http://www.immunityinc.com/documentation/ms08_001.html

- MS08-002 Faille dans LSASS
  - Affecte : Windows (toutes versions supportées sauf Vista)
  - Exploit : élévation de privilèges locale
  - Crédit : Thomas Garnier / SkyRecon (encore !)

Dernières vulnérabilités
Avis Microsoft (3/4)

- **Prévisions pour Février 2008**
  - **12 bulletins !**
    - **7 critiques : Windows (x2), VBScript / JScript, IE, Publisher, Office, Word**
    - **5 importants : Active Directory (DoS), Vista, IIS (x2 : élévation de privilèges et exécution de code à distance), Works**
- **Advisories**
  - **Q943411 Amélioration de la sécurité de la SideBar sous Vista**
    - **Blocage sélectif des gadgets possible**
  - **Q947563 Faille Excel inconnue exploitée dans la nature**
    - **Affecte : toutes versions supportées sauf Excel 2003 SP3, Excel 2007 et Excel 2008 pour Mac**

Dernières vulnérabilités
Avis Microsoft (4/4)

- Révisions
  - MS07-030
    - Version 1.1 : effet de bord documenté
  - MS07-042
    - Version 3.0 : Word Viewer 2003 est également affecté
  - MS07-057
    - Version 1.2 : effet de bord documenté
    - Version 1.3 : problème de mise en forme
  - MS07-061
    - Version 1.2 : effet de bord documenté
  - MS07-064
    - Version 1.3 : plus aucun effet de bord connu
    - Version 2.0 : DirectX 9.0 et 9.0b sont concernés
  - MS07-065
    - Version 1.3 : Windows XP Home n'est pas affecté
  - MS07-068
    - Version 1.2 : installer Windows Media Runtime 9.5 sur XP 64 bits
    - Version 1.3 : prise en compte de Windows 2003 64 bits
  - MS08-001
    - Version 2.0 : Windows SBS 2003 SP2 est affecté
    - Version 3.0 : requalification de l'impact sur SBS 2003 SP2 et Home Server

Dernières vulnérabilités
Infos Microsoft (1/6) - sorties

- Sorties logicielles
  - Windows 2008 et Windows Vista SP1 en RTM
    - 2008 dispo le 1er mars
    - SP1 dispo le 15 mars
  - SP1 pour le "pack de compatibilité Office 2007"
    - http://www.microsoft.com/downloads/details.aspx?FamilyId=9A1822C5-49C6-47BD-8BEC-0D68693CA564&displaylang=fr
  - SilverLight 1.0 poussé en "téléchargement facultatif" dans Microsoft Update
  - IE 7 poussé en "téléchargement obligatoire" dans Microsoft Update à partir du 12 février
    - http://support.microsoft.com/kb/946202/fr

Dernières vulnérabilités
Infos Microsoft (2/6) - sorties

- **Sorties logicielles**
  - **Gratuit pour les étudiants : Office 2007, Visual Studio 2005, SQL Server 2005, Virtual PC 2007**
    - **http://www.microsoft.com/france/etudiants/logiciels-gratuits/default.aspx**
  - **Nouvelle console d'administration de IIS 7**
    - **http://blogs.technet.com/longhorn/archive/2008/01/02/nouvelle-console-d-administration-d-iis-7-0-pour-vista-xp-et-windows-server-2003.aspx**
- **Et la sortie de Bill Gates …**
  - **http://video.msn.com/video.aspx?mkt=en-us&tab=soapbox&vid=be9075bb-df0a-41c9-8d86-7ded46627e26**

Dernières vulnérabilités
Infos Microsoft (3/6)

- Microsoft propose 44 milliards de dollars pour acquérir Yahoo
  - http://www.forbes.com/home/markets/2008/02/01/microsoft-yahoo-technology-markets-equity-cx_ll_0201markets10.html
  - Yahoo demande 56 Md$ …
- Le groupe des utilisateurs .NET sur … Second Life !
  - Bienvenue sur la Visual Studio Island
  - http://www.sldnug.net/
- Le groupe des utilisateurs .NET sur … Facebook !
- Le code source de .NET … presque une réalité
  - http://blogs.msdn.com/sburke/archive/2008/01/16/configuring-visual-studio-to-debug-net-framework-source-code.aspx

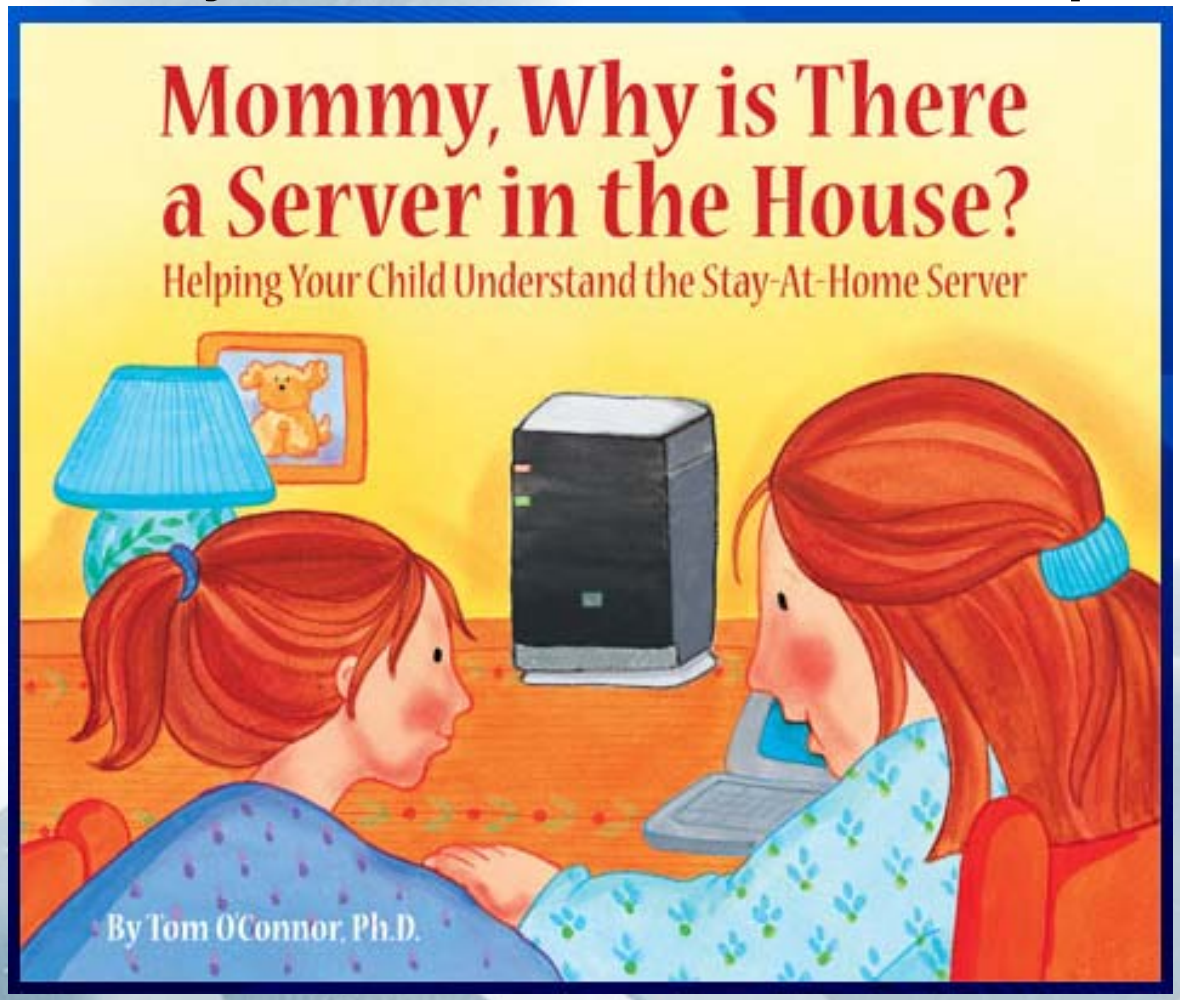
Dernières vulnérabilités
Infos Microsoft (4/6)

- Une bonne explication sur l'AutoRun
  - http://www.microsoft.com/technet/technetmag/issues/2008/01/SecurityWatch/default.aspx?loc=fr/

- La communication Microsoft
  - Hello Secure World
    - http://www.microsoft.com/click/hellosecureworld/default.mspx
  - Heroes Happen Here
    - http://blogs.technet.com/hhh_comic/default.aspx

Dernières vulnérabilités
Infos Microsoft (5/6)

- http://www.stayathomeserver.com/book.aspx



Dernières vulnérabilités
Infos Microsoft (6/6) - Vista

- Quelques nouveautés de Vista SP1
  - http://www.generation-nt.com/windows-vista-sp1-microsoft-refresh-actualite-66260.html
  - http://blogs.technet.com/markrussinovich/archive/2008/02/04/2826167.aspx
- Microsoft envoie des 'patchs' à des utilisateurs Vista non concernés...
  - http://www.silicon.fr/fr/news/2008/01/11/microsoft_envoie_des__patchs__a_des_utilisateurs_vista_non_concernes___
- Windows XP survivra-t-il au-delà du 30 juin 2008 ?
  - http://weblog.infoworld.com/save-xp/

Dernières vulnérabilités
Autres avis (1/10) – failles

"Les classiques" :

- Java 1.6 Update 4
  - Plus de 370 bugs corrigés
  - http://java.sun.com/javase/6/webnotes/ReleaseNotes.html#160_04
- QuickTime < 7.4
  - http://isc.sans.org/diary.html?storyid=3852
  - Au moins 4 failles de sécurité corrigées
- QuickTime < 7.4.1
  - Au moins 1 "heap overflow" corrigé
- Acrobat Reader < 8.1.2
  - Une faille de sécurité critique corrigée "silencieusement"
  - Mais exploitée dans la nature …
- FireFox 2.0.0.12
  - http://www.mozilla.org/projects/security/known-vulnerabilities.html#firefox2.0.0.12

Dernières vulnérabilités
Autres avis (2/10) – malwares et spam

- Une pratique de plus en plus courante : le *Domain Tasting*
  - Abus du délai de grâce par les *registrars*
  - Tout domaine peut être enregistré gratuitement pendant 5 jours
    - Utilisé dans les schémas "fast flux"
  - Network Solutions enregistre automatiquement toutes les recherches effectuées via son portail
    - http://www.dotsauce.com/2008/01/08/networksolutions-scandal-hijacking-domain-searches/
- Une application malicieuse pour iPhone (débloqué)
  - http://www.avertlabs.com/research/blog/index.php/2008/01/09/stay-on-main-street-for-iphone-apps/
  - "It was determined that the malicious repository and applications were created by an 11 year old. The child's parents were informed and the repository was taken down."

Dernières vulnérabilités
Autres avis (3/10) – malwares et spam

- Le premier "rogue antispyware" pour Mac
  - http://www.f-secure.com/weblog/archives/00001362.html
- Spam via un rebond sur Google
  - http://www.f-secure.com/weblog/archives/00001360.html
  - Evite les liens directs trop visibles
  - Note : Corbis est aussi de plus en plus utilisé pour charger des images …
- PowerShell : un futur vecteur d'infection ?
  - http://www.microsoft.com/technet/technetmag/issues/2008/01/PowerShell/default.aspx?loc=fr/
- Les auteurs de Storm identifiés par la police russe
  - Reste à les arrêter …
  - http://www.internetnews.com/ent-news/article.php/3724966

Dernières vulnérabilités
Autres avis (4/10) – malwares et spam

- Un bot en PHP
  - http://www.teamfurry.com/wordpress/2008/01/30/php-based-irc-botnet-fast-flux-of-course/
- Anti-Malware Testing Standards Organisation (AMSTO)
  - De nouveaux standards de test antivirus définis par les éditeurs
  - http://www.silicon.fr/fr/news/2008/02/05/securite___les_premiers_pas_de_l_amsto
- Les captchas sont vaincus par les russes
  - Yahoo!
    - http://network-security-research.blogspot.com/
  - Windows Live
    - http://www.websense.com/securitylabs/blog/blog.php?BlogID=171

Dernières vulnérabilités
Autres avis (5/10) – malwares et spam

- Le retour du rootkit de boot : Sinowal.A

  - Buzz
    - http://blogs.technet.com/pascals/archive/2008/01/11/oh-my-god-un-rootkit-dans-mon-mbr.aspx
    - http://www.avertlabs.com/research/blog/index.php/2008/01/24/new-wine-in-a-old-bottle-stealthmbr-rootkit/

  - Analyse technique
    - http://www2.gmer.net/mbr/

Dernières vulnérabilités
Autres avis (6/10) – attaques 2.0

- Défacements massifs par injection SQL automatisée
  - http://isc.sans.org/diary.html?storyid=3823
  - Le code malveillant est ajouté dans la base SQL, les pages du site ne sont pas modifiées
  - Computer Associate fait partie des victimes
    - http://techno.branchez-vous.com/actualite/2008/01/le_site_internet_de_ca_attaque.html
- A mettre en rapport avec :
  - Infections d'origine inconnue
    - http://www.theregister.co.uk/2008/01/11/mysterious_web_infection/
  - Compromission d'un service de publicité en ligne
    - http://www.pcworld.com/article/id,141358-c,techindustrytrends/article.html
  - 1 nouvelle page Web infectée toutes les 14 secondes
    - http://www.theregister.co.uk/2008/01/23/booby_trapped_web_botnet_menace/
  - Un site "Hacker Safe" piraté
    - http://www.vulnerabilite.com/hacker-safe-scanalert-mcafee-geeks-genica-piratage-vol-donnee-actualite-20080109032840.html

Dernières vulnérabilités
Autres avis (7/10) – attaques 2.0

- Une analyse très complète d'une attaque ciblée contre Falung Gong
  - http://www.daemon.be/maarten/targetedattacks.html
- Microsoft n'aime pas les applications qui exploitent la base Hotmail
  - 410 millions d'utilisateurs
  - Une pratique courante dans le Web 2.0 : donnez moi votre mot de passe que je puisse importer vos contacts
  - http://techland.blogs.fortune.cnn.com/2008/01/18/the-hard-side-of-mister-softie/
- Le prix d'une faille Windows aujourd'hui : $20,000
  - http://www.digitalarmaments.com/challenge200801566321.html
- Month of (Home) Router Bugs ?
  - http://www.gnucitizen.org/projects/router-hacking-challenge
- L'Asus EEE vulnérable "out of the box"
  - http://www.risesecurity.org/blog/entry/6/
  - Note : c'est un PC sous Linux ☺

Dernières vulnérabilités
Autres avis (8/10) – actualités

- Le gouvernement lance un portail "officiel" de la SSI
  - http://www.securite-informatique.gouv.fr/
  - http://www.ddm.gouv.fr/surfezintelligent/
- De nombreux câbles sous-marins endommagés en Méditerranée
  - http://www.renesys.com/blog/2008/01/mediterranean_cable_break.shtml
  - Impacte de nombreuses sociétés informatique "off-shore"
- TrueCrypt 5.0
  - Supporte le chiffrement intégral de disque
- Uninformed Volume 9
  - http://www.uninformed.org/?v=9

Dernières vulnérabilités
Autres avis (9/10) – just for fun

- "Google your password to see if it's good" ?
  - http://sunbeltblog.blogspot.com/2008/01/big-italian-bank-says-google-your.html
- Ne jamais virer son administrateur
  - http://www.generation-nt.com/yung-hsun-lin-medco-health-solutions-virus-jusitce-actualite-66272.html
  - http://www.foxnews.com/story/0,2933,325285,00.html
- Parfois il n'y a pas besoin de le virer
  - http://blogs.usatoday.com/ondeadline/2008/01/oops-cable-comp.html

Dernières vulnérabilités
Autres avis (10/10) – just for fun

- "The Great Zero Challenge"
  - http://16systems.com/zero/index.html
  - Qui va jouer pour … $100 ?
- Risquez sa vie pour son Iphone
  - http://laptopmag.com/Features/iPhone-Jumper.htm
- Le troll du mois
  - http://blogs.technet.com/pascals/archive/2007/12/14/petit-comparatif-amusant.aspx
  - http://blogs.technet.com/security/archive/2008/01/23/download-windows-vista-one-year-vulnerability-report.aspx
- Hervé Schauer sur … Facebook ☺

Dernières vulnérabilités
Autres infos (1/1)

- **Et pendant ce temps là sur la mailing liste de l'OSSIR**
  - **Spam et filtrage du port 25**
  - **Phishing en français**
  - **Que penser des certifications ?**
  - **Quelle implémentation Kerberos choisir ?**

Questions / réponses

- Questions / réponses
- Prochaine réunion le 10 mars 2008
- N'hésitez pas à proposer des sujets et des salles