OSSIR
Groupe Sécurité Windows

Réunion du 10 mars 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 (1/8)

- **Correctifs de Février 2008**
  - **Remarques**
    - **1 bulletin "critique" a disparu de la liste**
    - **Pas de correctif pour la faille Excel Q947563**
  - **MS08-003 Déni de service sur Active Directory & ADAM**
    - **Affecte : Windows 2000 Server, Windows 2003**
    - **Exploit :**
      - **Déni de service anonyme sur Windows 2000**
      - **Requière une authentification sur Windows 2003**
      - **Remplace MS07-039**
    - **Crédit : Thomas Garnier / SkyRecon**
  - **MS08-004 Déni de service sur TCP/IP**
    - **Affecte : Vista**
    - **Exploit : envoi d'une réponse DHCP malformée**
    - **Crédit : Tomas Potok & Martin Dominik & Martin Luptak & Eva Juhasova / WhiteStein**

Dernières vulnérabilités
Avis Microsoft (2/8)

- **MS08-005 Elévation de privilèges locale dans IIS**
  - **Affecte : IIS toutes versions supportées (IIS 5.0 -> 7.0)**
  - **Exploit : abus du mécanisme "File Change Notification"**
  - **Crédit : n/d**

- **MS08-006 Exécution de code à distance dans IIS**
  - **Affecte : IIS 5.1 et IIS 6.0**
  - **Exploit : envoi de données malformées à une page ASP**
    - **ASP n'est pas installé par défaut**
    - **Mais la faille reste critique !**
    - **https://strikecenter.bpointsys.com/articles/2008/02/13/exploiting-iis-via-htmlencode-ms08-006**
  - **Crédit : n/d**

Dernières vulnérabilités
Avis Microsoft (3/8)

- **MS08-007 Faille dans le redirecteur WebDAV**
  - **Affecte : Windows XP, 2003 et Vista**
  - **Exploit :**
    - ***heap overflow* en mode noyau en réponse à une requête WebDAV**
    - **Il existe un patch pour Samba permettant de déclencher le bogue**
    - **https://strikecenter.bpointsys.com/articles/2008/02/13/fun-with-webdav-ms08-007**
  - **Crédit : Steven / COSEINC**

- **MS08-008 Vulnérabilité dans OLE Automation**
  - **Affecte : Windows (toutes versions supportées) + Office 2004 pour Mac + Visual Basic 6 SP6**
  - **Exploit : *heap overflow***
  - **Crédit : Ryan Smith & Alex Wheeler / IBM ISS X-Force**

Dernières vulnérabilités
Avis Microsoft (4/8)

- MS08-009 Faille Word
  - Affecte : Office 2000, XP et 2003
  - Exploit : document Word malformé
  - Crédit : Rubén Santamarta / Reverse Mode

- MS08-010 Patch cumulatif pour IE (4 failles corrigées)
  - Affecte : IE (toutes versions supportées)
  - Exploit :
    - Faille dans le calcul du layout HTML
    - Faille dans une propriété HTML
    - Faille dans le passage d'arguments pour le rendu d'images
    - Faille dans l'ActiveX Fox Pro
  - Crédit :
    - Shane Macaulay & Riley Hassell / Security Objectives
    - TippingPoint & ZDI
    - Hyy / iDefense
    - VenusTech / AdLabs

Dernières vulnérabilités
Avis Microsoft (5/8)

- MS08-011 Failles dans le convertisseur Works (3 failles)
  - Affecte : Office 2003, Works 8.0, Works 2005
  - Exploit : fichier ".wps" malformé
    - http://www.milw0rm.com/exploits/5107
  - Crédit :
    - iDefense
    - Damian Put + iDefense
    - IBM ISS X-Force

- MS08-012 Failles dans Publisher (2 failles)
  - Affecte : Office 2000 / XP / 2003
  - Exploit : fichier ".pub" malformé
  - Crédit :
    - Piotr Bania
    - Bing Liu / Fortinet

Dernières vulnérabilités
Avis Microsoft (6/8)

- **MS08-013 Failles dans Office**
  - **Affecte : Office 2000 / XP / 2003 + Office 2004 pour Mac**
  - **Exploit : objet OLE malicieux dans un fichier Office**
  - **Crédit : Shaun Colley / NGSSoftware**

Dernières vulnérabilités
Avis Microsoft (7/8)

- Mise à jour "non sécurité"
  - Assistant de connexion Windows Live
    - http://support.microsoft.com/kb/947449
    - Qu'en pense Bruxelles ? ☺
- Prévisions pour Mars 2008
  - 4 failles Office allant jusqu'à "critique"
- Advisories
  - Aucun

Dernières vulnérabilités
Avis Microsoft (8/8)

- **Révisions**
  - **MS07-012**
    - **Version 2.1 : correction de la clé de base de registre**
  - **MS08-003**
    - **Version 1.1 : clé de base de registre incorrecte pour les versions 64 bits**
  - **MS08-005**
    - **Version 1.1 : lien de téléchargement pour les versions 64 bits incorrect**
  - **MS08-006**
    - **Version 1.1 : mise à jour de la liste des fichiers**
  - **MS08-007**
    - **Version 1.1 : interaction utilisateur nécessaire**
  - **MS08-008**
    - **Version 1.1 : le correctif VB6 SP6 remplace MS07-043**
    - **Version 1.2 : mise à jour des dates de fichiers**
  - **MS08-010**
    - **Version 1.1 : Vista SP1 et Windows 2008 ne sont pas affectés**
    - **Version 1.2 : correction de la clé de base de registre**
  - **MS08-012**
    - **Version 1.1 : pas de problème connu avec ce bulletin + typo**
  - **MS08-013**
    - **Version 1.1 : pas de problème connu avec ce bulletin**
    - **Version 1.2 : le correctif ne peut pas être désinstallé sur Office XP et 2003**

Dernières vulnérabilités
Infos Microsoft (1/7) - sorties

- **Sorties logicielles**
  - **Vista SP1 RTM**
    - **La liste des problèmes connus :**
      - **http://support.microsoft.com/kb/935796/en-us**
  - **Windows 2008**
    - **Lancement "mondial" le 27 février**
    - **Liste des changements :**
      - **http://4sysops.com/archives/new-features-in-windows-server-2008/**
  - **Exchange 2007 SP1 Rollup 1**
  - **SQL Server Data Services Beta**
    - **Projet pilote : Amazon S3**
    - **Accès Web à SQL Server**

Dernières vulnérabilités
Infos Microsoft (2/7) - sorties

- IE 8 Beta1
  - http://www.microsoft.com/windows/products/winfamily/ie/ie8/default.mspx
  - "Features" pour la sécurité :
    - Domain Highlighting
    - Contournement possible de la Same Origin Policy
  - IE 8 sera compatible "au plus proche" des standards du Web
    - http://www.microsoft.com/presspass/press/2008/mar08/03-03WebStandards.mspx
    - http://blogs.msdn.com/ie/archive/2008/03/05/internet-explorer-8-beta-1-for-developers-now-available.aspx
  - Un pas vers l'Open Source ?
    - Suites de test sous licence BSD
    - Bugtracker public
    - http://blogs.msdn.com/ie/archive/2008/03/06/ie8-and-ip-licensing.aspx

Dernières vulnérabilités
Infos Microsoft (3/7) - sorties

- Et surtout … Microsoft publie toutes ses spécifications librement et gratuitement !
  - Introduction :
    - http://msdn2.microsoft.com/en-us/library/cc216514.aspx
  - Explication :
    - http://www.microsoft.com/presspass/press/2008/feb08/02-21ExpandInteroperabilityPR.mspx
    - http://blogs.technet.com/porte25/archive/2008/02/21/nouveaux-principes-d-interop-rabilit.aspx
  - Formats Office :
    - http://www.microsoft.com/interop/docs/OfficeBinaryFormats.mspx
  - Protocoles réseau :
    - http://msdn2.microsoft.com/en-us/library/cc216517.aspx

Dernières vulnérabilités
Infos Microsoft (4/7)

- L'initiative SafeCode … pour du code plus sûr ?
  - http://www.safecode.org/
  - Consortium dans lequel Microsoft est partie prenante
- Un Quiz sécurité à destination des PME
  - http://www.microsoft.com/smallbusiness/support/quiz/quizquestions.mspx
- Microsoft Research réfléchit aux "vers correcteurs"
  - http://technology.newscientist.com/article/dn13318-friendly-worms-could-spread-software-fixes.html
- Microsoft Research : HD View
  - http://research.microsoft.com/ivm/hdview.htm
  - Aucun rapport avec la sécurité ☺
- Pour les alpha-testeurs de SilverLight 1.1
  - http://www.andybeaulieu.com/silverlight/DestroyAll/Default.html

Dernières vulnérabilités
Infos Microsoft (5/7)

- Microsoft se rapproche des idées du Jericho Forum
  - http://www.itrmanager.com/articles/73324/bernard-ourghalian-direction-technique-securite-microsoft-br-nouvelle-vision-securite-microsoft-1ere-partie.html
- F# : un langage de type fonctionnel sur la machine .NET
  - http://msdn.microsoft.com/msdnmag/issues/08/LA/FSharpIntro/default.aspx
- Récupérer le code source du framework .NET
  - http://www.codeplex.com/NetMassDownloader
- Windows Seven
  - http://blogs.technet.com/longhorn/archive/2008/02/19/quelques-liens-sur-windows-7.aspx

Dernières vulnérabilités
Infos Microsoft (6/7) - Vista

- "Petit" problème lors de la dernière mise à jour Vista
  - http://isc.sans.org/diary.html?storyid=3998
- Vista SP1 ne corrige pas la "faille" de la reconnaissance vocale
  - http://blogs.zdnet.com/security/?p=875
- Une mise à jour pas comme les autres …
  - http://support.microsoft.com/kb/940510
- Vista et les firewalls
  - http://support.microsoft.com/kb/934430

Dernières vulnérabilités
Infos Microsoft (7/7) - Vista

- **Vista SpringBoard**
  - Pour répondre à des questions essentielles telles que :
    - "Windows XP me suffit. Pourquoi changer ?"
    - "Quel est l'intérêt de Windows Vista ?"
  - http://technet.microsoft.com/fr-fr/windowsvista/bb905048.aspx

- **Communiqué de presse Microsoft : les ventes de Vista sont bonnes**
  - 400,000 PCs équipés de Vista vendus chaque mois
  - http://www.microsoft.com/france/CP/2008/1/2008013001_a208.mspx

Dernières vulnérabilités
Autres avis (1/13) – failles

- Thunderbird 2.0.0.12
  - Corrige 5 failles dont 1 critique
  - Remarques :
    - La branche 1.x n'est plus supportée
    - 3 semaines avant de communiquer sur cette faille …
    - Opera (également vulnérable) a été notifié 24h avant la publication de la faille …
      - http://forums.acbm.com/acbm/forum/viewthread?thread=923
    - Le patch est incomplet …
      - http://www.0x000000.com/index.php?i=515

- Une faille mal patchée dans VMWare
  - Affecte : Workstation, Player et ACE
  - Exploit : "directory traversal" dans les dossiers partagés
    - http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1004034
  - Crédit : CORE

Dernières vulnérabilités
Autres avis (2/13) – failles

- Une bonne collection de failles Access (14 en tout)
  - http://seclists.org/fulldisclosure/2008/Feb/0314.html
  - Microsoft ne considère pas ces failles comme "critique" car Access ne fait pas partie de Office Standard

Dernières vulnérabilités
Autres avis (3/13) – malwares et spam

- Le groupe 29A, c'est fini …
  - http://vx.org.ua/29a/main.html
- 11 Chinois arrêtés pour vol de mot de passe
  - Opéraient sur le réseau chinois "Tencent QQ"
  - http://www.avertlabs.com/research/blog/index.php/2008/02/14/when-is-stealing-not-theft/
- Google : 1,3% du Web mondial est pourri
  - http://research.google.com/archive/provos-2008a.pdf
- Recrutement massif de "mules" au Canada
  - Au Canada, il est possible de transférer des fonds uniquement avec une adresse email
  - http://www.f-secure.com/weblog/archives/00001385.html

Dernières vulnérabilités
Autres avis (4/13) – malwares et spam

- FTC : rapport annuel sur la fraude et le vol d'identité
  - http://www.ftc.gov/opa/2008/02/fraud.pdf
- Un marché des logins FTP volés
  - http://www.darkreading.com/document.asp?doc_id=147123&WT.svl=news2_1
- Le rootkit MBR, c'est du sérieux
  - Quelques fonctions :
    - Distribution "dans la nature"
    - Mises à jour par l'auteur
    - Obfuscation
    - Fonctions réseau
    - Non détection
    - Le pire reste à venir … ?
  - http://www.f-secure.com/weblog/archives/00001393.html

Dernières vulnérabilités
Autres avis (5/13) – malwares et spam

- Le *captcha* de GMail cassé à son tour
  - Une organisation complexe et structurée
  - http://www.websense.com/securitylabs/blog/blog.php?BlogID=174
- 17 personnes arrêtées au Canada dans une opération anti-botnets
  - … dont 1 femme
  - 1 million de PCs contrôlés
  - http://www.canada.com/calgaryherald/news/story.html?id=f0f6138c-0bd7-4061-bb8e-be7d6d4b654d
- Un malware Chinois rançonne les utilisateurs de portable
  - 50 "QQ coins" pour débloquer l'équipement
  - http://www.avertlabs.com/research/blog/index.php/2008/03/04/crimeware-goes-mobile/
- McAfee publie SAGE n°3
  - http://www.mcafee.com/us/research/sage/sage_2008_linkpage.html

Dernières vulnérabilités
Autres avis (6/13) – actualités

- Beaucoup de bruit autour de la nouvelle "Google Toolbar"
  - Modifie la page retournée en cas d'erreur 404
  - http://googlewebmastercentral.blogspot.com/2007/12/fyi-on-google-toolbars-latest-features.html
- Quand AES == XOR …
  - http://it.slashdot.org/it/08/02/19/0213237.shtml
- Un portable acheté sur eBay contenait un CD "confidentiel"
  - Caché sous le clavier !
  - http://news.sky.com/skynews/article/0,,30100-1307259,00.html

Dernières vulnérabilités
Autres avis (7/13) – actualités

- La rémanence de la RAM fait du bruit
  - L'étude :
    - http://citp.princeton.edu/memory/
    - http://citp.princeton.edu.nyud.net/pub/coldboot.pdf
    - http://www.youtube.com/watch?v=JDaicPIgn9U
  - Le buzz :
    - http://www.nytimes.com/2008/02/22/technology/22chip.html?ex=1204347600&en=b927c3d99483b842&ei=5070&emc=eta1
  - La réponse des vendeurs :
    - TrueCrypt :
      - http://www.truecrypt.org/docs/?s=unencrypted-data-in-ram
    - BitLocker :
      - http://blogs.msdn.com/windowsvistasecurity/archive/2008/02/22/disk-encryption-balancing-security-usability-and-risk-assessment.aspx
    - http://isc.sans.org/diary.html?storyid=4024

Dernières vulnérabilités
Autres avis (8/13) – actualités

- **Adam Boileau distribue son outil d'attaque via FireWire**
  - **http://storm.net.nz/static/files/winlockpwn**
  - **http://www.theage.com.au/news/security/hack-into-a-windows-pc-no-password-needed/2008/03/04/1204402423638.html**

- **Le projet SandMan passe dans le domaine public**
  - **Objectif : lecture du fichier d'hibernation Windows**
  - **http://www.msuiche.net/2008/02/26/sandman-10080226-is-out/**

- **L'US Air Force achète 300 PlayStation 3**

Dernières vulnérabilités
Autres avis (9/13) – actualités

- Le plan de la cyber-police française
  - http://www.zdnet.fr/actualites/internet/0,39020774,39378623,00.htm
    - Préparation de la LOPSI
    - Cyber-perquisition (y compris à l'étranger)
      - Déjà autorisé en Allemagne :
      - http://forums.acbm.com/acbm/forum/viewthread?thread=933
    - Recrutement et formation des policiers avec l'aide d'organismes privés
    - Point de contact pour le signalement des contenus illicites
    - Commission de déontologie

Dernières vulnérabilités
Autres avis (10/13) – actualités

- Encore une panne du réseau BlackBerry
  - http://isc.sans.org/diary.html?storyid=3970
  - http://feeds.feedburner.com/Bb-outage
  - Ca ne fait plus autant recette qu'avant …
- Les 15 "hackers" les plus influent aujourd'hui
  - http://www.eweek.com/c/a/Security/The-15-Most-Influential-People-in-Security-Today/
  - Totalement subjectif ☺
- Décès de "Dude Van Winkle" à l'âge de 31 ans
  - http://www.timesreporter.com/index.php?ID=79446&r=6&Category=7
- Bill Gates n'est plus l'homme le plus riche du monde
  - http://www.lefigaro.fr/votrepatrimoine/2008/03/06/05010-20080306ARTFIG00364-bill-n-est-plus-l-hommele-plus-riche-du-monde.php

Dernières vulnérabilités
Autres avis (11/13) – actualités

- Le 12 février : le jour de l'Internet plus sûr
  - http://www.saferinternet.org/ww/en/pub/insafe/index.htm
  - Pas grand chose en France

- 56% des utilisateurs pensent qu'Internet a été plus sûr en 2007 qu'en 2006 …
  - http://www.baselinemag.com/c/a/Security/Survey-Users-Believe-Internet-Is-Safer/

- BackStopp : l'autodestruction à base de RFID
  - http://backstopp.com/

- eBay Belgique : s'authentifier avec sa carte d'identité ?
  - http://www.reseaux-telecoms.net/actualites/lire-en-belgique-ebay-proposera-la-carte-d-identite-electronique-comme-moyen-d-identification-des-internautes-17770.html

Dernières vulnérabilités
Autres avis (12/13) – actualités

- Les interfaces clavier/terminal de certains lecteurs de CB "sniffables"
  - http://news.bbc.co.uk/1/hi/programmes/newsnight/7265437.stm
  - Note : les anglais ont toujours été réfractaire au code PIN …
- VMWare prépare quelquechose dans le domaine de la sécurité
  - http://www.vmware.com/overview/security/vmsafe.html
  - Suite au rachat de Determina ?
- Le "FUD" du mois
  - Le matériel fabriqué en Asie "pourrait" être backdooré
    - http://www.pcpro.co.uk/news/173883/chinese-backdoors-hidden-in-router-firmware.html
    - http://www.thetrumpet.com/index.php?q=4524.2780.0.0
    - http://www.govexec.com/story_page.cfm?articleid=38713&dcn=todaysnews

Dernières vulnérabilités
Autres avis (13/13) – just for fun

- Spam + Art =
  - http://iradlee.net/spamology/
- "Tiger Team" : la sécurité fait toujours rêver
  - http://www.trutv.com/video/?id=870&link=truTVshlk
- Le problème de la Cyber-Guerre aux USA
  - http://www.wired.com/politics/security/news/2008/02/cyber_command?currentPage=all
- Le nouveau téléphone à la mode : Nokia Morph
  - http://www.nokia.com/A4630650?category=rd
- Le cerveau du rat reconstitué en laboratoire
  - http://www.seedmagazine.com/news/2008/03/out_of_the_blue.php?page=all&p=y
- Gary Gygax est mort ☹

Dernières vulnérabilités
Autres infos (1/1)

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

  - Failles dans le produit IPDiva
  - Plages d'adresses IP des particuliers
  - Extraction de clés depuis la mémoire vive ("cold boot" attack)
  - CSS 3 et sécurité
  - Machines à voter
  - Mise à disposition des spécifications des protocoles Microsoft

Questions / réponses

- Questions / réponses
- Prochaine réunion le 7 avril 2008
- N'hésitez pas à proposer des sujets et des salles