OSSIR
Groupe Sécurité Windows

Réunion du 11 juin 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 (1/12)

- **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 (2/12)

- **Correctifs de Avril 2007**
  - **MS07-017**
    - **Correctif pour la faille ANI …**
    - **… et bien plus !**
      - **http://blogs.technet.com/photos/pcfs-gallery/images/725076/original.aspx**
  - **MS07-018 Failles multiples dans Microsoft CMS**
    - **Affecte : Microsoft CMS 2001 SP1, CMS 2002 SP2**
    - **Exploit : buffer overflow, cross-site scripting**
    - **Crédit : Martyn Tovey / Netcraft**
  - **MS07-019 Faille UPnP**
    - **Affecte : Windows XP SP2**
    - **Exploit : buffer overflow**
      - **A priori non exploitable si DEP est actif**
    - **Crédit : Greg MacManus / iDefense Labs**

Dernières vulnérabilités
Avis Microsoft (3/12)

- **MS07-020 Faille dans Microsoft Agent**
  - **Affecte : Windows (toutes versions supportées) - sauf Vista**
  - **Exploit : URL malformée (???)**
  - **Crédit : JJ Reyes and Carsten Eiram of Secunia**

- **MS07-021 Failles multiples dans CSRSS**
  - **Affecte : Windows (toutes versions supportées) – y compris Vista**
  - **Exploit : DoS ou élévation de privilèges**
    - **Faille NtRaiseHardError()**
    - **Faille ApiPort – spécifique à Vista (introduction des ALPC)**
  - **Crédits : Tim Garnett / Determina, eEye**

Dernières vulnérabilités
Avis Microsoft (4/12)

- MS07-022 Faille noyau
  - Affecte : Windows 2000 SP4, Windows XP SP2 32-bit, Windows 2003 SP0/SP1/SP2
  - Exploit : élévation locale de privilèges (permissions incorrectes sur un segment partagé)
  - Crédit : eEye

Mai 2007

- MS07-023 Failles multiples dans Excel
  - Affecte : Excel 2000 / 2002 / 2003 / 2007 + Excel 2004 pour Mac
    - Mais pas Works
  - Exploit : corrige 3 failles permettant d'exécuter du code
  - Crédit :
    - Manuel Santamarina Suarez + ZDI
    - Greg MacManus / iDefense

Dernières vulnérabilités
Avis Microsoft (5/12)

- MS07-024 Failles multiples dans Word
  - Affecte : Word 2000 / 2002 / 2003 + Word 2004 pour Mac + Works
    - Mais pas Word 2007
  - Exploit : corrige 3 failles permettant d'exécuter du code
    - Exploité "dans la nature"
  - Crédit :
    - Craig Schmugar / McAfee
    - Andreas Marx / AVTest
    - iDefense

- MS07-025 Faille dans Office
  - Affecte : Office 2000 / 2002 / 2003 / 2007 + Office 2004 pour Mac
    - Composants : Excel, Frontpage, Publisher, Expression, SharePoint Designer
  - Exploit : corrige une faille permettant d'exécuter du code
  - Crédit : N/D

Dernières vulnérabilités
Avis Microsoft (6/12)

- MS07-026 Failles multiples dans Exchange
  - Affecte : Exchange 2000 / 2003 / 2007
  - Exploit : corrige 4 failles
    - 2 dénis de service
    - 1 exécution de script
    - 1 exécution de code via un email malformé
  - Crédit :
    - Martijn Brinkers / Izecom
    - Alexander Sotirov / Determina
    - Joxean Koret + iDefense

Dernières vulnérabilités
Avis Microsoft (7/12)

- MS07-027 Patch cumulatif pour Internet Explorer
  - Affecte : IE toutes versions supportées (y compris Vista)
  - Exploit : corrige 5 failles et tue ("kill bit") 4 (?) contrôles ActiveX
    - {D9998BD0-7957-11D2-8FED-00606730D3AA}
      - Support Acer
    - {1D95A7C7-3282-4DB7-9A48-7C39CE152A19}
      - "Research In Motion TeamOn Import Object"
  - Crédit :
    - ZDI
    - JJ Reyes / Secunia
    - Cocoruder/ Fortinet

Dernières vulnérabilités
Avis Microsoft (8/12)

- **MS07-028 Faille dans CAPICOM**
  - **Affecte : BizTalk Server 2004 + redistribuable CAPICOM**
  - **Exploit : exécution de code via le contrôle ActiveX CAPICOM**
  - **Crédit : Chris Ries / Vigilant Minds**

- **MS07-029 Faille dans le service DNS**
  - **Affecte : Windows 2000 Server, Windows 2003**
  - **Exploit : exécution de code à distance via les outils d'administration DNS distante (sur RPC)**
    - **Largement exploité dans la nature (Q935964)**
  - **Crédit :**
    - **Mark Hofman / SANS**
    - **Bill O'Malley / Carnegie Mellon**

Dernières vulnérabilités
Avis Microsoft (9/12)

- **Juin 2007**
  - **4 failles "critiques" affectant Windows**
  - **1 faille "moyenne" affectant Visio**
  - **1 faille "mineure" affectant Windows**

Dernières vulnérabilités
Avis Microsoft (10/12)

- Advisories
  - Q935423 → MS07-017
  - Q935964 → MS07-029
    - Affecte : Windows 2000 Server, Windows 2003
    - Exploit : faille de sécurité dans le service RPC "Serveur DNS"
      - Exploitée "dans la nature" en "0day"
  - Q937696 Publication de "MOICE" et "File Block"
    - Un bac à sable pour Office 2003 et Office 2007
  - Q927891 Problèmes dans le service Windows Installer
    - "Sans conséquence pour la sécurité"
    - Mais les problèmes suivants sont rencontrés sur WindowsUpdate
      - CPU à 100%
      - "Access violation" dans SVCHOST
      - "Memory leak"
      - Durée de la mise à jour > 1h

Dernières vulnérabilités
Avis Microsoft (11/12)

- Révisions
  - MS05-026
    - Version 1.2 : oubli du bulletin MS02-055 dans la liste des mises à jour intégrées (!)
  - MS05-032
    - Version 2.1 : bulletin redistribué car non cumulatif avec MS06-068
  - MS05-043
    - Version 1.2 : ajout d'un lien vers Q908506
  - MS06-068
    - Version 1.1 : ce bulletin n'est pas cumulatif avec MS05-032
  - MS07-004
    - Version 1.2 : IE 7 installé sur Windows 2003 SP2 *est* vulnérable
  - MS07-005
    - Version 1.1 : patch à appliquer sur Windows 2003 SP2 également
  - MS07-012
    - Version 1.2 : précisions sur l'édition de liens statiques
  - MS07-018
    - Version 1.1 : problèmes d'incompatibilité

Dernières vulnérabilités
Avis Microsoft (12/12)

- **MS07-020**
  - **Version 1.1 : mise à jour de la liste des fichiers sous Windows 2003**
  - **Version 1.2 : correction sur Windows 2003 64-bit**
- **MS07-021**
  - **Version 1.1 : mise à jour de la liste des fichiers**
- **MS07-023**
  - **Version 1.1 : mise à jour d'un nom de fichier**
  - **Version 1.2 : nouvelles incompatibilités détectées**
- **MS07-025**
  - **Version 1.1 : Word Viewer est *aussi* affecté**
  - **Version 1.2 : nouvelles incompatibilités détectées**
- **MS07-027**
  - **Version 1.1 : mise à jour de la liste des fichiers**
  - **Version 1.2 : plusieurs typos et incompatibilités**
  - **Version 1.3 : correction sur Windows 2003 64-bit**
- **MS07-029**
  - **Version 1.1 : le service DNS doit être installé avant le patch**
  - **Version 1.2 : correction sur Windows 2003 64-bit**

Dernières vulnérabilités
Infos Microsoft (1/4)

- Microsoft Security Intelligence Report, second semestre 2006
  - Plus de vulnérabilités … mais plus complexes à exploiter
  - Rbot est la souche la plus détectée "in the wild"
  - Les failles Office ne sont exploitées que dans des attaques ciblées
  - La suite :
    - http://download.microsoft.com/download/f/d/a/fda5850e-269f-40a3-9708-c60eb837456f/MS_Security_Report_Jul-Dec06.pdf

- Sorties logicielles
  - LongHorn Beta3
    - http://www.microsoft.com/winme/0704/29897/Beta_3_Video_2_MBR.asx
  - SilverLight CTP
  - SilverLight 1.0 Beta SDK
  - SilverLight 1.1 Alpha SDK (très fort !)
  - .NET Framework 3.5 Beta1
  - Visual Studio "Orcas", incluant "Language Integrated Query" (LINQ)
  - MultiPoint SDK (pour avoir plusieurs souris :)
  - Windows Mobile Device Center 6.1 (pour Vista)
  - … et tant d'autres …

Dernières vulnérabilités
Infos Microsoft (2/4)

- Microsoft fait son *mea-culpa* après la faille ANI
  - http://blogs.msdn.com/sdl/archive/2007/04/26/lessons-learned-from-the-animated-cursor-security-bug.aspx
  - Microsoft envisage de bannir memcpy()
  - Pas de protection de pile
    - Le compilateur n'a pas vu le *buffer* de taille variable
    - => "/GS" plus agressif dans la prochaine version de Visual Studio
  - SafeSEH et ASLR inefficaces
    - Nombre d'essais illimité grâce au gestionnaire d'exceptions
  - Faille non détectée en *fuzzing*
    - Le bug était dans le *deuxième* entête "anih"

Dernières vulnérabilités
Infos Microsoft (3/4)

- **Attention**
  - **Le support de Windows 2003 SP0 a expiré en avril 2007**

- **Microsoft Desktop Optimization Pack for Software Assurance**
  - **Contient :**
    - **Softricity SoftGrid**
    - **AssetMetrix**
    - **Winternals IT Admin Pak**
    - **Desktop Standard GPOVault**
  - **https://partner.microsoft.com/40033588**

Dernières vulnérabilités
Infos Microsoft (4/4)

- TechNet Mag de juin consacré à Vista et la sécurité
  - http://www.microsoft.com/technet/technetmag/issues/2007/06/default.aspx?loc=fr
- Microsoft Surface : le PC du futur ?
  - http://www.microsoft.com/surface/
- Microsoft PhotoSynth : tout simplement incroyable …
  - http://labs.live.com/photosynth/
- MVP, une position pas si enviable …
  - http://www.theregister.com/2007/06/05/microsoft_mvp_threats/
- Philippe Gildas y croit
  - http://tempsreel.nouvelobs.com/actualites/economie/entreprises/20070605.OBS0400/philiippe_gildas_attaquemicrosoft_en_justice.html
  - Arnold Schwarzenegger va s'y mettre aussi ? ;)

Dernières vulnérabilités
Autres avis (1/7) – failles

- Java 6 Update 1 (avril 2007)

- Faille VMWare
  - Affecte : VMWare < 5.5.4
  - Exploit : *directory traversal* dans les dossiers partagés
  - Crédit : Greg MacManus / iDefense

- Faille Quicktime
  - Affecte : QuickTime < 7.1.6
  - Exploit : *heap overflow* dans le traitement des applets Java
  - Crédit : Dino Dai Zovi
  - Remarques :
    - Faille critique exploitée lors du concours "Pwn 2 Own" (CanSecWest 2007)
    - Egalement vendue $10,000 à iDefense

Dernières vulnérabilités
Autres avis (2/7) – failles

- "0day" WinAmp
  - Affecte : Winamp < 5.34
  - Exploit : faille dans le traitement des fichiers MP4

- *Buffer overflow* à l'ouverture d'un projet VB 6.0
  - Affecte : Visual Basic 6.0 (Visual Studio 6.0)
  - Exploit : http://www.milw0rm.com/exploits/3977
  - Remarque : le fuzzing Visual Studio semble être à la mode …

- Déni de service via les fichier ".ICO"
  - Affecte : Windows XP
  - Exploit : déréférencement d'un pointeur NULL via un fichier malformé
    - http://www.csis.dk/dk/forside/GdiPlus.pdf

Dernières vulnérabilités
Autres avis (3/7) – failles

- Il va falloir mettre à jour son téléphone plus souvent …
  - http://www.symantec.com/enterprise/security_response/weblog/2007/06/access_violations_on_windows_c.html
- Déni de service (réseau local)
  - Affecte : Vista
  - Exploit :
    - Paquet ARP qui coupe toutes les interfaces
      - Exploitable sur le LAN uniquement
    - http://www.milw0rm.com/exploits/3926
- Toutes les applications Vista ne sont pas compatibles IPv6 …
  - http://www.networkworld.com/news/2007/060707-microsoft-vista-ipv6-incompatible.html

Dernières vulnérabilités
Autres avis (4/7) – failles Web

- La mode des « Month of X Bug »
  - Month of Browser Bugs (été 2006) par HD Moore
  - Month of Kernel Bugs (novembre 2006) par HD Moore
  - Month of Apple Bugs (janvier 2007) par LMH and Kevin Finisterre
  - Month of PHP Bugs (Mars 2007) par Stefan Esser
  - Month of MySpace Bugs (avril 2007) par Mondo Armando et Müstaschio (seulement 17 jours de découvertes de failles)
  - Month of ActiveX Bugs (mai 2007) par shinnai

  Et…

  - Month of Search Engines Bugs (juin 2007) par Mustive
    - http://websecurity.com.ua/category/moseb/

Dernières vulnérabilités
Autres avis (5/7) – failles Web

- Le filtre anti-XSS du moteur ASP.NET contournable
  - Affecte : ASP.NET 2.0
  - Exploit : </XSS/*-*/STYLE=xss:e/**/xpression(alert('XSS'))>
    - Ne fonctionne que sur un client Internet Explorer
  - Crédit : http://www.procheckup.com/Vulner_PR0703.php

- Les sites "de confiance" n'existent plus
  - Ex. asus.com infecté par la faille ANI
    - http://www.viruslist.com/en/weblog?weblogid=208187358
  - Ex. un sous-domaine de "ieak.microsoft.com" défacé
    - http://isc.sans.org/diary.html?storyid=2699

Dernières vulnérabilités
Autres avis (6/7) – virus et spywares

- Un virus curieux
  - Infecte les iPod "reflashés" sous Linux
    - http://www.viruslist.com/en/weblog?weblogid=208187356
- Le virus Jowspry.A utilise BITS pour contourner les firewall personnels
  - http://www.microsoft.com/security/portal/Entry.aspx?ThreatId=-2147383707
- eEye Labs présente un rootkit "matériel"
  - Basé sur le firmware extensible de la carte réseau Tigon2
  - http://www.eeye.com/html/resources/newsletters/vice/VI20070425.html
- Les "scams 419" deviennent agressifs (menaces de mort) !
  - http://isc.sans.org/diary.html?storyid=2771
- Les tendances du spam depuis 2000
  - http://www.stearns.org/spamreport/spamreport.html

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

- Encore des failles dans les antivirus
  - Security Center de McAfee (10/05/07)
  - F-Secure (31/05/07)
  - Symantec Enterprise Security Manager (29/05/07)

Dernières vulnérabilités
Autres infos (1/6)

- Une intrusion profonde dans les systèmes américains
  - … suite à un "0day" Office très ciblé
    - http://www.usatoday.com/tech/news/computersecurity/2007-04-22-cyberspies-microsoft-office_N.htm
- Les frères Kumar annoncent avoir "cassé" les TPM
  - http://lists.immunitysec.com/pipermail/dailydave/2007-May/004335.html
- "Google Apps Partner Edition"
  - Une version "standalone" principalement destinée aux FAI
  - Faut-il commencer à avoir peur ?
- Idée géniale ou flop annoncé ?
  - http://www.signal-spam.fr/
  - A lire avant d'acheter :
    - http://forums.acbm.com/acbm/forum/viewthread?thread=583

Dernières vulnérabilités
Autres infos (2/6)

- Rapport de l'agence suisse MELANI
  - Les attaques utilisant de l'ingénierie sociale augmentent
  - Les attaques ciblées et le vol d'information augmentent
  - Les réseaux se structurent
    - Recherche de faille / écriture d'attaques => exploitation => blanchiment
  - Lire la suite :
    - http://www.melani.admin.ch/dokumentation/00123/00124/01019/index.html?lang=fr

- McAfee publie un rapport sur les Data Breaches
  - "Datagate: The Next Inevitable Corporate Disaster?"
    - http://www.mcafee.com/us/enterprise/products/promos/data_loss_protection/default.html
  - Dommage car eux-mêmes en ont été victimes ;)
    - http://www.privacyrights.org/ar/ChronDataBreaches.htm

Dernières vulnérabilités
Autres infos (3/6)

- Delphi 2007 supporte NX et ASLR
  - http://www.codegear.com/
- Panne de routeur géante au Japon
  - A priori une erreur humaine
  - http://www.networkworld.com/news/2007/051607-cisco-routers-major-outage-japan.html
- Le NIST propose un format XML pour la description des check-lists de sécurité
  - XCCDF - The Extensible Configuration Checklist Description Format
  - http://nvd.nist.gov/scap/xccdf/xccdf.cfm
- "Office of Management and Budget" impose une configuration de sécurité unique à tous les postes de l'administration US
  - http://www.govexec.com/dailyfed/0307/032007p2.htm

Dernières vulnérabilités
Autres infos (4/6)

- **Microsoft invite les chercheurs en sécurité au BlueHat**
  - **http://www.microsoft.com/technet/security/bluehat/2007spring.mspx**

- **La fin des DRM : iTunes, VirginMega, Starzik**
  - **http://www.ratiatum.com/breve5121_Starzik_propose_a_son_tour_EMI_sans_DRM_VirginMega_aussi_MAJ.html**

- **Drive By Download – les internautes toujours aussi crédules ?**
  - **http://didierstevens.wordpress.com/2007/05/07/is-your-pc-virus-free-get-it-infected-here/**

Dernières vulnérabilités
Autres infos (5/6)

- La sécurité : un marché de 7 milliards de dollars en 2006
  - http://solutions.journaldunet.com/dossiers/chiffres/virus.shtml
- Le Web 3.0 est en marche …
  - http://www.neojobmeeting.com/
- Le téléchargement P2P surveillé à partir de 50 fichiers partagés en 24h !
  - http://www.dematériel.com/2007/06/01/telechargement-illegal-la-decision-du-conseil-detat-ouvre-la-voie-a-la-riposte-graduee/
- La publicité en ligne pas toujours bien maîtrisée ☺

Dernières vulnérabilités
Autres infos (6/6)

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

  - **Liste SUR**
    - **Sécurité Messagerie (secret des correspondances)**
    - **Possibilité de SNAT IP avec un bridge netfilter**
    - **Passerelle d'échanges sécurisés**
    - **Sécurité du poste client (connexion à l'entreprise depuis un poste personnel)**

  - **Liste NT**
    - **Rien ☹**

Questions / réponses

- Questions / réponses
- Date de la prochaine réunion
  - Prochaine réunion le 9 juillet 2007
- N'hésitez pas à proposer des sujets et des salles