OSSIR
Groupe Sécurité Windows

Réunion du 7 avril 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

- **Correctifs de Mars 2008**

  - **MS08-014 Failles multiples dans Excel (x7)**
    - **Affecte :**
      - **Excel 2000 SP3, Excel XP SP3, Excel 2003 SP2, Excel 2007**
      - **Excel Viewer 2003, pack de compatibilité 2007, Office pour Mac (2004 et 2008)**
    - **N'affecte pas :**
      - **Excel 2003 SP3, Excel 2007 SP1**
    - **Exploit :**
      - **Corruption mémoire via des fichiers ".xls" ou ".slk" malformés**
      - **Injection de commandes**
      - **Exécution de macros sans confirmation**
      - **Etc.**

Dernières vulnérabilités
Avis Microsoft

- Crédit :
  - Mike Scott / SAIC
  - Matt Richard / VeriSign
  - Greg McManus / iDefense
  - Anonyme via iDefense
  - Yoshiya Sasaki / JFE Systems
  - Bing Liu / Fortinet
  - Cody Pierce / TippingPoint
  - Moti Joseph, Dan Hubbard / WebSense
- Détails :
  - L'une des failles était exploitée "dans la nature" avant le patch
    - Advisory Q947563
  - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=671
  - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=672
  - Version 2.0 du patch presque immédiatement disponible

Dernières vulnérabilités
Avis Microsoft

- **MS08-015 Faille dans Outlook**
  - **Affecte : toutes versions supportées sauf Office 2007 SP1**
  - **Exploit : passage de commandes dans un tag "mailto:"**
  - **Crédit : Greg McManus / iDefense**
  - **Détails :**
    - **http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=673**

- **MS08-016 Failles multiples dans Excel (x2)**
  - **Affecte : Excel 2000 SP3, Office XP SP3, Office 2003 SP2, Excel Viewer 2003, Office 2004 pour Mac**
  - **Exploit : corruption mémoire**
  - **Crédit :**
    - **Arnaud Dovi via ZDI**
    - **Anonyme**

Dernières vulnérabilités
Avis Microsoft

- **MS08-017 Failles multiples dans Office Web Components (x2)**
  - **Affecte :**
    - **Office 2000 SP3, Office XP SP3**
    - **Visual Studio 2002 SP1, Visual Studio 2003 SP1**
    - **BizTalk Server 2000 et 2002**
    - **Commerce Server 2000**
    - **ISA Server 2000 SP2**
  - **Exploit : corruption mémoire**
    - **La faille la plus ancienne a été documentée en 2006 ! (CVE-2006-4695)**
  - **Crédit :**
    - **Chris Ries / VigilantMinds Inc.**
    - **Xiao Hui of NCNIPC**
    - **Yuval Ben-Itzhak / Finjan**

Dernières vulnérabilités
Avis Microsoft

- Mise à jour "non sécurité"
  - Extensions de GPO (voir plus loin)

- Prévisions pour Avril 2008
  - 8 bulletins
    - 5 critiques : 1x Office, 2x Windows, 2x Windows+IE
    - 3 importants : 1x Office, 2x Windows

- Advisories
  - Q950627 Faille dans "Microsoft Jet Database Engine"
    - Exploitable via un document Office
      - Tout document Office est capable d'ouvrir silencieusement un fichier Access quelle que soit son extension
    - Windows 2003 SP2 et Vista ne sont pas affectés
      - Faille corrigée silencieusement ?
    - Connue depuis 2005
      - http://research.eeye.com/html/alerts/zeroday/20050331.html

Dernières vulnérabilités
Avis Microsoft

- **Révisions**
  - **MS07-021**
    - **Version 1.2 : ajout de problèmes connus**
  - **MS07-025**
    - **Version 2.0 : les packs de compatibilité Office 2007 sont également affectés**
  - **MS07-040**
    - **Version 2.0 : .NET 1.0 et 1.1 sont affectés sur Vista SP1 et Windows 2008**
  - **MS08-003**
    - **Version 1.2 : ajout d'un article de KB sur les problèmes connus**

Dernières vulnérabilités
Avis Microsoft

- MS08-014
  - Version 1.1 : une mise à jour est disponible pour une version non vulnérable d'Office (!)
  - Version 2.0 : erreur de calcul ☺
    - http://support.microsoft.com/kb/950340
  - Version 3.0 : de nouveaux problèmes corrigés ...
- MS08-015
  - Version 1.1 : une mise à jour est disponible pour une version non vulnérable d'Office (!) + mise à jour de la liste des fichiers
  - Version 1.2 : mise à jour de la liste des fichiers Outlook 2000
- MS08-016
  - Version 1.1 : une mise à jour est disponible pour une version non vulnérable d'Office (!) + correctif non inclus dans Office XP SP3
  - Version 1.2 : remplace MS07-025
- MS08-017
  - Version 1.1 : correction des liens et clés de base de registre
  - Version 1.2 : ajout d'un lien vers CVE

Dernières vulnérabilités
Infos Microsoft - sorties

- **Sorties logicielles**
  - **IE 8 Beta 1**
    - **IE 5.5 : vainqueur du test ACID 3 ?**
      - **http://www.anomalousanomaly.com/2008/03/06/acid-3/**
  - **Windows Vista SP1 sur Windows Update**
    - **Liste des pilotes incompatibles**
      - **http://www.guwiv.com/portal/blogs/news/archive/2008/03/20/vista-sp1-la-liste-des-pilotes-qui-posent-probl-232-me.aspx**
      - **Inclus Symantec 11.0**
      - **Le Service Pack n'est pas déployé si l'un de ces pilotes est détecté**
  - **Hyper-V RC0**
  - **SilverLight 2 Beta 1**
    - **Avec la technologie "Deep Zoom"**

Dernières vulnérabilités
Infos Microsoft - sorties

- Les extensions de GPO poussées dans Windows Update
  - http://support.microsoft.com/kb/943729
    - Permet de contrôler par GPO par exemple :
    - Folder options
    - Mapped drives
    - Printers
    - Scheduled tasks
    - Services
    - Start menu settings

- Autres sorties
  - Windows Server 2008 Security Guide

Dernières vulnérabilités
Infos Microsoft

- Vous avez toujours voulu comprendre comment fonctionne Windows ?
  - http://www.academicresourcecenter.net/curriculum/FacetMain.aspx?FT=Tag&TagList=13&ResultsTitle=Operating%20Systems&ShowResults=1
  - Et particulièrement :
    - http://www.academicresourcecenter.net/curriculum/pfv.aspx?ID=6191
- MFC version 2008 en préparation
  - http://blogs.msdn.com/somasegar/archive/2007/11/09/visual-c-libraries-update.aspx
- Méchant troll détecté ☺
  - http://www.microsoft.com/windowsserver/compare/default.mspx
  - En particulier :
    - http://www.microsoft.com/windowsserver/compare/webcasts/Windows-UAC-compared-to-Linux-Sudo.mspx

Dernières vulnérabilités
Infos Microsoft

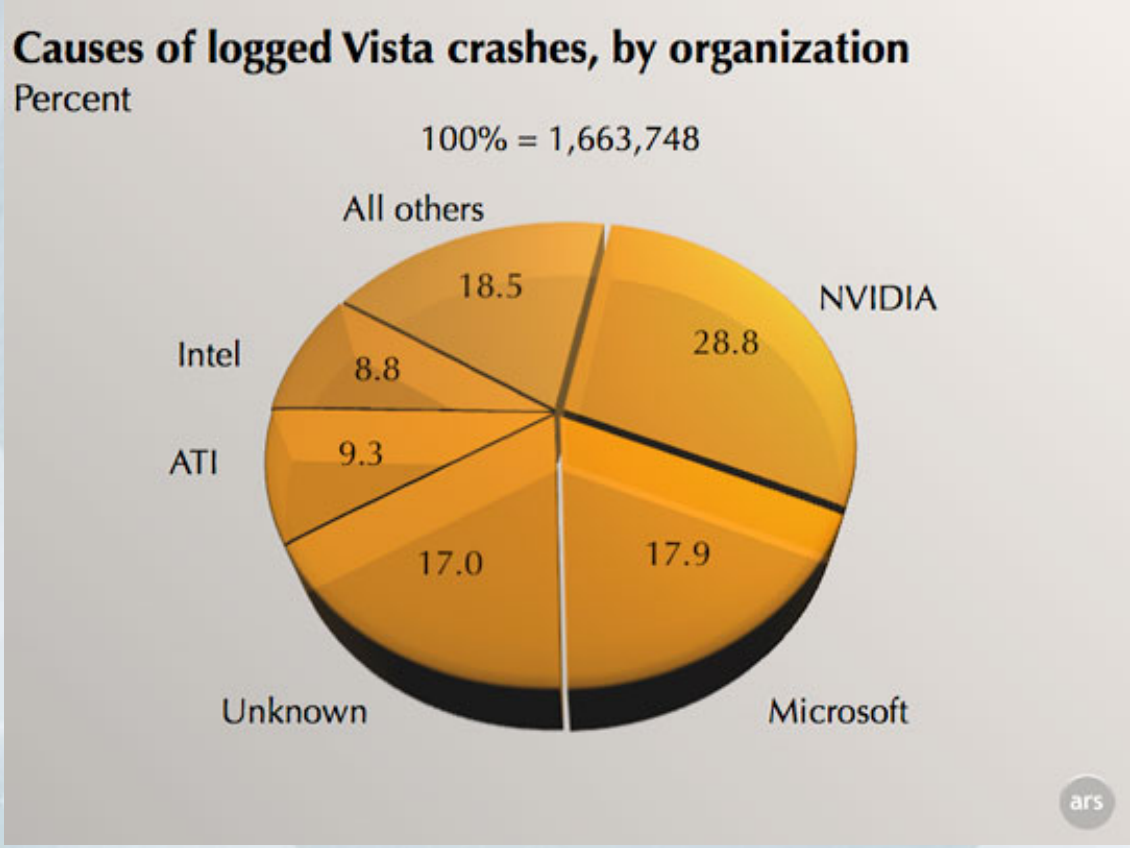
- Bientôt une certification "Windows Internals" chez Microsoft ?
  - http://blogs.msdn.com/ntdebugging/archive/2008/03/21/wanted-windows-internals-subject-matter-experts.aspx
- Les vidéos "How do I ?"
  - http://msdn2.microsoft.com/en-us/security/bb896640.aspx
- Microsoft achète Komoku
  - http://www.komoku.com/
- Microsoft DreamSpark
  - Gratuit pour les étudiants :
    - Windows 2003 Server Standard
    - Visual Studio 2005 et 2008 Pro
    - SQL Server 2005 Developer Edition
    - Expression Studio
    - XNA Game Studio 2.0

Dernières vulnérabilités
Infos Microsoft - Vista

- Les applications tierce-partie : le talon d'Achille de Vista
  - http://erratasec.blogspot.com/2008/02/unsafe-at-anyspeed.html
- Pourtant tout est expliqué ici :
  - http://msdn2.microsoft.com/en-us/magazine/cc337897.aspx
- L'erreur qui tue
  - http://support.microsoft.com/?kbid=946084
    - *"If you have only one disk installed, and if you have access to Windows XP or Windows 2000 installation media, restart the computer by using the Windows XP or Windows 2000 installation media. Next, format the offending disk, and then reinstall Windows Vista."*

Dernières vulnérabilités
Infos Microsoft - Vista

- Pourquoi Vista plante ?



- http://arstechnica.com/news.ars/post/20080325-vista-capable-lawsuit-paints-picture-of-buggy-nvidia-drivers.html

Dernières vulnérabilités
Autres avis – failles

- Faille d'injection de commandes dans un lien "ftp://"
  - Affecte : IE 5 et IE 6
  - Exploit :
    - "ftp://user@site:port/%0D%0ADELE%20foo.txt%0D%0A//"
    - http://www.rapid7.com/advisories/R7-0032.jsp
  - Correctif : IE 7

- FireFox 2.0.0.13
  - Corrige plusieurs failles "critiques"

- Nombreux avis de sécurité Adobe
  - Date de publication : 11 mars 2008
  - http://www.adobe.com/support/security/

- Déni de service dans les MFC si le nom de processus ne contient pas de '.'
  - http://malwareanalysis.com/CommunityServer/blogs/geffner/archive/2008/03/26/986.aspx

Dernières vulnérabilités
Autres avis – failles

- Failles multiples dans VMWare
  - Versions non affectées :
    - VMware Workstation 6.0.3
    - VMware Workstation 5.5.6
    - VMware Player 2.0.3
    - VMware Player 1.0.6
    - VMware ACE 2.0.3
    - VMware ACE 1.0.5
    - VMware Server 1.0.5
    - VMware Fusion 1.1.1

- Nouvelle suite de fuzzing des formats d'archive
  - http://www.ee.oulu.fi/research/ouspg/protos/testing/c10/archive/
  - Et les nombreuses failles qui en découlent ...
    - Antivirus : F-Secure, ...
    - Logiciels de décompression : WinRar, 7-Zip, Bzip2, Unzip, ...

Dernières vulnérabilités
Autres avis – failles

- Failles multiples dans Safari
  - Affecte : Safari < 3.1
  - Des failles dans la 3.1 ont déjà été trouvées ☺
    - http://www.heise-online.co.uk/security/Two-vulnerabilities-in-Windows-Safari--/news/110395
  - D'ailleurs ...
    - ... la première machine du concours Pwn2Own / CanSecWest 2008 est tombée grâce à une faille dans WebKit !
    - C'est un Mac ☺
  - Et aussi ...
    - Le contrat de licence Safari pour Windows interdit l'installation sur du matériel non-Apple ☺
    - http://apple.slashdot.org/article.pl?sid=08/03/27/129236
- Opera et Safari font 100% au test ACID 3

Dernières vulnérabilités
Autres avis – failles

- Quelques failles Opera pour faire bonne figure
  - http://www.opera.com/support/search/view/881/
  - http://www.opera.com/support/search/view/882/

- Failles multiples dans QuickTime < 7.4.5
  - Au moins 11 failles corrigées

Dernières vulnérabilités
Autres avis – malwares et spam

- 2 comparateurs d'antivirus s'associent
  - "Anti Malware Test Lab" et "AV Comparatives"
    - Une réponse à l'Anti-Malware Testing Working Group ?
    - A noter que les tests sont payants pour les éditeurs de produits
  - Les antivirus restent contestés ...
    - http://blogs.the451group.com/security/?p=16

- Plus de 10,000 sites compromis d'un seul coup
  - http://isc.sans.org/diary.html?storyid=4139
  - IFRAME malicieuse située sur le site "2117966.net"
  - 2 cibles principales => 2 gangs ?
    - 13,000 pages ASP
    - 200,000 pages phpBB
  - Démo :
    - http://www.vimeo.com/moogaloop.swf?clip_id=781981

- Une combinaison JavaScript + VBScript intéressante
  - http://isc.sans.org/diary.html?storyid=4231

Dernières vulnérabilités
Autres avis – malwares et spam

- BluePill passe la seconde
  - http://theinvisiblethings.blogspot.com/2008/03/kick-ass-hypervisor-nesting.html
- Le patron d'un gang de *carding* se présente aux élections en Ukraine
  - Son programme : lutter contre la corruption …
  - http://blog.washingtonpost.com/securityfix/2008/03/ukranian_cybercrime_boss_leads.html
- Malware et Art
  - http://www.sq.ro/malwarez.php
- The S.P.A.M. Experiment
  - Objectif : acheter les produits proposés par du spam
  - http://www.mcafeespamexperiment.com/

Dernières vulnérabilités
Autres avis – attaques 2.0

- Le site de Trend Micro piraté
  - http://www.dslreports.com/forum/r20161397-Trend-Micro-Hacked-Serving-Malicious-Iframes
- Une intrusion très ciblée "numéros de CB"
  - http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9073138&pageNumber=1
- 6,000 CVs de Harvard volés lors d'une intrusion
  - Le fichier s'est rapidement retrouvé sur BitTorrent …
  - http://www.news.harvard.edu/gazette/2008/03.13/99-hacked.html
- 5,000 données personnelles volées à MTV
  - ... par un cheval de Troie très simple
  - http://www.lesnouvelles.net/articles/attaques/mtv-se-fait-voler-les-donnees-de-5000-employes

Dernières vulnérabilités
Autres avis – attaques 2.0

- LinkedIn propose désormais des profils d'entreprise
  - http://blog.linkedin.com/blog/2008/03/company-profile.html
- Après le Month of Router Bugs, un ver D-Link ?
  - Scan SNMP + Telnet
  - http://isc.sans.org/diary.html?storyid=4175
- Trouver la langue d'une conversation VoIP en analysant la distribution du trafic ?
  - http://www.cs.jhu.edu/~cwright/voip-vbr.pdf
- Augmentation significative des attaques ciblées contre les activistes Tibétains
  - Envoi de fichiers malformés avec du contenu sensé
  - Formats DOC, XLS, PPT, PDF, ...
  - Vol de keyrings PGP
  - http://isc.sans.org/diary.html?storyid=4177

Dernières vulnérabilités
Autres avis – attaques 2.0

- L'achat/vente de "0day", trop long à conclure ?
  - http://snosoft.blogspot.com/2008/03/exploit-acquisition-program-shut-down.html
- L'outil DaisyDukes pour extraire des mots de passe en mémoire
  - Présenté à CanSecWest 2008 mais non disponible publiquement
  - http://www.theregister.co.uk/2008/03/28/memory_sniffer_unveiled/
- E-Trade annonce $18 million de fraude pour Q1 2008
  - http://www.rootkit.com/blog.php?newsid=866
- L'outil Goolag pour auditer son site Web
  - http://goolag.org/
  - Egalement disponible depuis ce lien ☺
    - http://go.microsoft.com/?linkid=8601222

Dernières vulnérabilités
Autres avis – actualités

- Le SDK iPhone disponible
  - Lien officiel :
    - http://developer.apple.com/iphone/program/
  - Une fausse bonne affaire :
    - http://www.techcrunch.com/2008/03/07/iphone-sdk-some-of-the-details-arent-great/

- Le Sectéra Edge : un SmartPhone pour la NSA
  - http://www.gdc4s.com/content/detail.cfm?item=32640fd9-0213-4330-a742-55106fbaff32
  - Sous Windows Mobile

- Concours Pwn2Own 2008 (conférence CanSecWest)
  - Mac OS X exploité via une faille Safari
  - Vista exploité via une faille Flash + Java
  - Ubuntu non exploité (mais la faille Flash marcherait)

  - http://cansecwest.com/post/2008-03-20.21:33:00.CanSecWest_PWN2OWN_2008

Dernières vulnérabilités
Autres avis – actualités

- L'ENISA publie un document sur le Risk Management
  - http://www.enisa.europa.eu/rmra/h_home.html
- Gratuité de tous les *proceedings* Usenix
  - http://www.usenix.org/publications/library/proceedings/
- Demain (8 avril 2008)
  - Rencontres parlementaires à la Maison de la Chimie
  - "Les nouveaux titres sécurisés : enjeux et technologies de demain"

Dernières vulnérabilités
Autres avis – just for fun

- Hacker un *pacemaker* ?
  - http://www.secure-medicine.org/icd-study/icd-study.pdf
  - Communication sans-fil avec l'équipement
- Comment gérer un "databreach" quand on utilise une technologie anti-"databreach" ...
  - http://securitywatch.eweek.com/disaster_planning/hannaford_data_breach_the_security_vendor_conundrum.html
- Un Trivial Pursuit version ITIL
  - http://www.01net.com/editorial/363817/le-trivial-pursuit-est-disponible-en-version-itil/
  - D'autres normes sont en préparation ...

Dernières vulnérabilités
Autres avis – just for fun

- Le jour où il est impossible d'aller sur Internet : le 1er avril
  - Google est particulièrement créatif
    - http://mail.google.com/mail/help/customtime/index.html
    - http://www.google.com/virgle/index.html
    - http://www.google.com.au/intl/en/gday/index.html
  - InfoWorld également
    - http://www.infoworld.com/article/08/04/01/14FE-april-fool-google-us-gov_1.html
    - http://www.infoworld.com/article/08/04/01/14FE-april-fool-security-study_1.html

Questions / réponses

- Questions / réponses
- JSSI le 22 mai 2008
- Prochaine réunion le 9 juin 2008
- N'hésitez pas à proposer des sujets et des salles