OSSIR
Groupe Sécurité Windows

Réunion du 13 juin 2005

Revue des dernières vulnérabilités Microsoft

Nicolas RUFF

nicolas.ruff@eads.net

Dernières vulnérabilités
Avis Microsoft (1/6)

- (Avis de sécurité Microsoft depuis le 11 avril 2005)

- Avril 2005
- Bulletins "critiques"
  - MS05-019 Vulnérabilités TCP/IP (x5 !)
    - Affecte : au minimum Windows 2000 / XP / 2003
    - Exploit :
      - Exécution de code à distance (?)
      - "Land Attack" (IPv4)
      - Réinitialisation de connexion via un paquet ICMP "destination unreachable"
      - Injection de données dans une session TCP en utilisant une faille dans la gestion des Timestamps TCP et l'option PAWS (Protection Against Wrapped Sequence Numbers)
    - Crédit :
      - Song Liu, Hongzhen Zhou, Neel Mehta (ISS X-Force)
      - Ainsi que : Fernando Gont, Qualsys

Dernières vulnérabilités
Avis Microsoft (2/6)

- MS05-020 Patch cumulatif pour IE
  - Exploit : exécution de code via DHTML, des fichiers "Content Advisor", ou des URL malformées
    - Ex. "race condition" dans createElement(), appendChild(), removeNode()
  - Crédit :
    - Berend-Jan Wever, 3APA3A, axle@bytefall + iDefense
    - Andres Tarasco (SIA Group)
- MS05-021 Vulnérabilité Exchange
  - Affecte : Exchange 2000 SP3, 2003, 2003 SP1
  - Exploit : "buffer overflow" dans une commande SMTP
  - Crédit : Mark Dowd, Ben Layer (ISS X-Force)
- MS05-022 Vulnérabilité MSN
  - Affecte : MSN Messenger 6.2
  - Exploit : "buffer overflow" exploitable via un GIF malformé
  - Crédit : Hongzhen Zhou
- MS05-023 Vulnérabilité Word (x2)
  - Affecte : Word 2000 / XP / 2003 (et Works 2001 – 2004)
  - Exploit : "buffer overflow" à l'ouverture d'un document
  - Crédit : Alex Li

Dernières vulnérabilités
Avis Microsoft (3/6)

- **Bulletins "importants"**
  - **MS05-016 Vulnérabilité dans le shell Windows**
    - **Affecte : Windows 2000 SP3/SP4, Windows XP SP1/SP2, Windows 2003**
    - **Exploit : un fichier OLE est ouvert en fonction de son CLSID et non de son extension**
    - **Crédit : iDefense**
  - **MS05-017 Vulnérabilité dans MSMQ**
    - **Affecte : Windows 2000 SP3/SP4, Windows XP SP1**
    - **Exploit : "buffer overflow" exploitable via RPC**
    - **Crédit : Kostya Kortchinsky**
  - **MS05-018 Vulnérabilités Kernel (x4)**
    - **Affecte : Windows 2000 SP3/SP4, Windows XP SP1/SP2, Windows 2003**
    - **Exploit : local uniquement (élévation de privilèges, DoS)**
      - **4 problèmes identifiés, dont 1 concernant la gestion des polices par le noyau**
    - **Crédit :**
      - **John Heasman + NGSSoftware**
      - **Sanjeev Radhakrishnan, Amit Joshi, Ananta Iyengar + GreenBorder**
      - **David Fritz + iDefense**

Dernières vulnérabilités
Avis Microsoft (4/6)

- **Révisions**
  - **MS05-002**
    - **Version 2.0 : corrige le problème avec Windows 98/ME**
  - **MS05-009**
    - **Version 2.0 : installation incorrecte par SUS**
    - **Version 2.1 : précision sur Messenger 4.7 / XP SP1**
    - **Version 2.2 : déploiement de la version 4.7**
    - **Version 2.3 : paramètres en ligne de commande pour la version 4.7**
  - **MS05-010**
    - **Version 1.2 : prise en compte de l'exploitation anonyme**
  - **MS05-017**
    - **Version 1.1**
  - **MS05-019**
    - **Version 1.1 : régressions détectées, le patch sera republié en Juin**
      - **Ex. Windows 2003 SP1 : perte de paquets sur des liens ayant des MTU différentes**
  - **MS05-021**
    - **Version 1.1**
  - **MS05-022**
    - **Version 1.1 : précision sur Messenger 6.2**
  - **MS05-023**
    - **Version 1.2 : procédure pour le déploiement automatisé du patch**
    - **Version 1.3 : typo dans la version Word 2000**

Dernières vulnérabilités
Avis Microsoft (5/6)

- **Mai 2005**
- **Bulletin "important"**
  - **MS05-024 Vulnérabilités dans la prévisualisation de documents via EXPLORER**
    - **Affecte : Windows 2000 (versions supportées : SP3, SP4)**
    - **Exploitation :**
      - **La conversion en tags "mailto:" ne filtre pas les scripts dans le nom de l'auteur**
      - **http://www.greymagic.com/security/advisories/gm015-ie/**

Dernières vulnérabilités
Avis Microsoft (6/6)

- "Microsoft Security Advisories"
  - Q892313 : Exécution de scripts sans confirmation dans WMP via le DRM
    - Affecte : Windows Media Player 9 et 10
  - Q842851 : "Tarpitting" SMTP
    - Utilisable avec Exchange 2003 + Windows 2003 SP1
    - Clé "TarpitTime"
  - Q899480 : Réinitialisation des connexions TCP à travers les "timestamps" TCP
    - Corrigé par MS05-019
- Juin 2005
  - 7 bulletins Windows (allant jusqu'à Critique)
  - 1 bulletin Windows / SFU (Modéré)
  - 1 bulletin Exchange (Important)
  - 1 bulletin ISA Server (Modéré)

Dernières vulnérabilités
Infos Microsoft (1/3)

- **Journées Microsoft de la Sécurité Informatique**
  - 14 et 15 juin au CNIT
  - http://go.microsoft.com/?linkid=2785082
  - http://go.microsoft.com/?linkid=2785097
- **Le "GateKeeper Test 2005"**
  - Du 2 au 12 mai, 2 questions par jour
  - http://go.microsoft.com/?linkid=2785098
  - Mais le test a été annulé car des petits malins ont trouvé le moyen de tricher ☺
- **Windows 2003 SP1 AdminPack**
  - http://go.microsoft.com/?linkid=2945288
- **Windows 2003 R2 en Beta publique**
  - http://go.microsoft.com/?linkid=3024749
- **"Windows Server 2003-based computer becomes slow and unresponsive after running for several days" ☺**
  - http://support.microsoft.com/kb/821008/

Dernières vulnérabilités Infos Microsoft (2/3)

- Des problèmes fixés silencieusement dans 2003 SP1
  - "Buffer overflow" dans la gestion des chemins UNC
    - http://www.securityfocus.com/bid/12969
  - DoS via le redirecteur SMB
    - http://www.securityfocus.com/bid/13008
- Windows XP supporte WPA2
  - http://support.microsoft.com/?id=893357
- Visual Studio 2005 remplace toutes les fonctions "dangereuses" de la LibC par une version "safe"
  - http://go.microsoft.com/?linkid=2896730
  - Ex. wcscpy() -> wcscpy_s()
- Nouveautés dans la sécurité de SQL Server 2005
  - http://go.microsoft.com/?linkid=3024796
- Chiffrement complet du disque avec Longhorn + TPM 1.2
  - http://go.microsoft.com/?linkid=2896734

Dernières vulnérabilités
Infos Microsoft (3/3)

- Un nouveau service : "Microsoft Security Advisories"
  - Pour les avis de sécurité "pas si graves que ça"
    - Inclus les 0day vus dans la nature …
  - http://go.microsoft.com/fwlink/?LinkId=47489
  - http://news.com.com/Microsoft+to+sound+early+alert+for+flaws/2100-1002_3-5697945.html
- Passage des formats Office en XML
  - .DOC -> .DOCX, .XLS -> .XLSX, .PPT -> .PPTX
  - Spécifications libres et publiques
  - http://go.microsoft.com/?linkid=3253444
- Nouveautés en avant-première
  - Exchange 2003 SP2
  - SQL Server 2005 (prévu le 7 novembre 2005)
  - Visual Studio 2005 (prévu le 7 novembre 2005)

Dernières vulnérabilités
Autres avis (1/4)

- Des choses qu'on lit encore en 2005 …
  - http://news.bbc.co.uk/1/hi/technology/3485972.stm
  - "It's a myth that hackers find the holes, said Nigel Beighton" (Symantec)
- Le projet "Polaris" chez HP
  - http://www.hpl.hp.com/techreports/2004/HPL-2004-221.html
  - Encore un moniteur comportemental pour Windows
- L'utilisation des "raw sockets" provoque un "kernel panic"
  - Affecte : Windows XP SP1
  - http://www.securityfocus.com/bid/12870
- IPv6 dans Windows est toujours vulnérable à la Land Attack
- Il est possible d'éteindre un PC à distance avec TSShutdn.exe
  - Affecte : Windows XP SP1
  - http://www.securityfocus.com/bid/12889

Dernières vulnérabilités
Autres avis (2/4) - virus

- Le premier spyware "open source"
  - http://nzeka-labs.com/hacking/KSpyware.htm
  - Quelques dizaines de lignes en PERL
  - Fait par un français …
- Nopir-B : un virus (français) qui détruit les fichiers illégaux !
  - http://www.sophos.com/virusinfo/articles/nopirb.html
- Une Lexus infectée par un virus BlueTooth ?
  - Source : Kaspersky
  - http://www.lesnouvelles.net/articles/virus/641-automobiles-lexus-virus-bluetooth.html
- Problème dans l'analyse des fichiers RAR par Symantec AV
  - http://securityresponse.symantec.com/avcenter/security/Content/2005.04.27.html
- Toujours une forte activité virale
  - Sober.P

Dernières vulnérabilités
Autres avis (3/4) - navigateurs

- "0day" dans FireFox
  - Affecte : FireFox 1.0.3
  - Exploit : exécution automatique de code binaire téléchargé depuis Internet, via un javascript mal filtré
    - Fonction vulnérable : l'installeur d'extensions
  - Remarques :
    - Une solution temporaire a été apportée par Mozilla Foundation en ajoutant des caractères aléatoires aux extensions
    - Visiblement il y aurait eu une fuite via BugZilla
- DoS
  - Affecte : IE toutes versions
  - Exploit : une balise onLoad() fait crasher IE
  - Crédit : Benjamin Tobias Franz

Dernières vulnérabilités
Autres avis (4/4)

- "Windows Genuine Advantage" cracké …
  - http://www.hackingspirits.com/vuln-rnd/defeating-wga-check.zip
  - http://www.xillioncomputers.com/modules.php?name=News&file=article&sid=336
  - http://news.com.com/Bypass+found+for+Windows+piracy+check/2100-1002_3-5717127.html?tag=st_lh
- "Microsoft Windows OneCare"
  - Support antivirus et antispyware payant
  - Pas très bien accueilli par les utilisateurs …
    - http://news.zdnet.co.uk/internet/security/0,39020375,39198263,00.htm
- Apple migre vers processeur x86 …

Questions / réponses

- Questions / réponses
- Date de la prochaine réunion
  - Lundi 11 juillet 2005
- N'hésitez pas à proposer des sujets et des salles