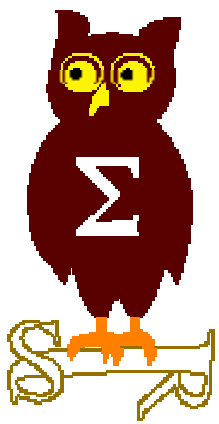
OSSIR
Groupe Sécurité Windows

Réunion du 7 novembre 2005



Revue des dernières vulnérabilités Microsoft

Nicolas RUFF

EADS-CCR

nicolas.ruff@eads.net

Dernières vulnérabilités
Avis Microsoft (1/5)

- (Avis de sécurité Microsoft depuis le 10 octobre 2005)

- Octobre 2005
  - MS05-044 : "directory traversal" dans le client FTP
    - Affecte : IE 6 SP1
    - Exploit : un serveur malicieux renvoie un nom de fichier de la forme "../fichier"
  - MS05-045 : DoS local sur les connexions réseau via la "connection manager"
    - Affecte : Windows 2000 SP4, Windows XP SP1/SP2, Windows 2003 SP0/SP1
    - Exploit : N/D

Dernières vulnérabilités
Avis Microsoft (2/5)

- MS05-046 "Buffer Overflow" dans le service client NetWare
  - Affecte : Windows 2000 SP4, Windows XP SP1/SP2, Windows 2003 SP0/SP1
  - Exploit : exécution de code à distance (note : le service NetWare n'est pas démarré par défaut)
  - Crédit : Kostya Kortchinsky

- MS05-047 "Buffer Overflow" dans le service PnP
  - Affecte : Windows 2000 SP4, Windows XP SP1/SP2
  - Exploit : exécution de code à distance (requière une authentification sous Windows XP)
  - Crédit : eEye (Derek Soeder)

- MS05-048 "Buffer Overflow" dans CDO (Collaborative Data Objects)
  - Affecte : Windows 2000 SP4, Windows XP SP1/SP2, Windows 2003 SP0/SP1, Exchange 2000 SP3
  - Exploit : exécution de code à distance
  - Crédit : Gary O'leary-Steele

Dernières vulnérabilités
Avis Microsoft (3/5)

- MS05-049 Vulnérabilités multiples dans l'interface Windows
  - Affecte : Windows 2000 SP4, Windows XP SP1/SP2, Windows 2003 SP0/SP1
  - Exploit :
    - 2 vulnérabilités dans le support des fichiers .LNK
    - 1 vulnérabilité dans l'aperçu WebView
  - Crédit : Cesar Cerrudo / Brett Moore

- MS05-050 "Buffer Overflow" dans DirectShow
  - Affecte : DirectX 7.0 – 9.0c
  - Exploit : exécution de code arbitraire à l'ouverture d'un fichier .AVI
  - Crédit : eEye (Fang Xing)

- MS05-051 Vulnérabilités multiples dans COM+ et DTC
  - Affecte : Windows 2000 SP4, Windows XP SP1/SP2, Windows 2003 SP0/SP1
  - Exploit :
    - "Buffer Overflow" dans COM+ exploitable à distance
    - "Buffer Overflow" dans DTC exploitable à distance
    - Utilisation de DTC comme zombie pour DoS (via IDENTIFY)
    - DoS dans DTC
  - Crédit : eEye, iDefense, Cesar Cerrudo

Dernières vulnérabilités
Avis Microsoft (4/5)

- **MS05-052 Vulnérabilités multiples dans IE**
  - **Affecte : IE 5.01 SP4, IE 5.5 SP2, IE 6.0, IE 6.0 SP1**
  - **Exploit : "Buffer Overflow" multiples lors de l'initialisation de composants ActiveX**
  - **Crédit : Will Dormann, FrSIRT, Parvez Anwar, eEye (Fang Xing)**

- **Advisories**
  - **Q909444 : problèmes recensés avec MS05-051 si le répertoire %WINDIR%\registration n'a pas les permissions par défaut**

- **Novembre**
  - **1 bulletin critique affectant Windows**

Dernières vulnérabilités
Avis Microsoft (5/5)

- **Révisions**
  - **MS05-038**
    - **Version 2.2 : les "monikers" ne sont plus supportés dans IE**
  - **MS05-045**
    - **Version 1.1 : description de la clé de base de registre pour Windows 2003**
  - **MS05-050**
    - **Version 1.1 : clarifications de la description**
    - **Version 1.2 : clarifications de la description**
    - **Version 1.3 : détails sur les interactions avec DirectX**
  - **MS05-051**
    - **Version 1.1 : problèmes de permissions décrits ci-dessous**
  - **MS05-052**
    - **Version 1.1 : clarifications de la description**
    - **Version 1.2 : description de la clé de base de registre pour Windows 2003**
    - **Version 1.3 : incompatibilité entre différents niveaux de protection**

Dernières vulnérabilités
Infos Microsoft (1/2)

- Les futures Stock Control Unit (SKU) de Longhorn …
  - Windows Vista Starter
  - Windows Vista Home Basic
  - Windows Vista Home Premium
  - Windows Vista Ultimate
  - Windows Vista Pro Standard/SB
  - Longhorn Enterprise Server (ADS)
  - Longhorn Enterprise Server - IA64
  - Longhorn Standard Server
  - Longhorn Datacenter Server
  - Windows Vista Pro Std/SB/Ent - VL Binding Service
  - Windows Vista Pro Std/SB/Ent – VLGeneric
  - Windows Vista Pro Std/SB/Ent – DMAK
  - Windows Vista Starter Digital Boost – OEM
  - Windows Vista Home Basic – OEM
  - Windows Vista Home Premium – OEM
  - Windows Vista Ultimate – OEM
  - Windows Vista Pro Standard/SB – OEM
  - Longhorn Enterprise Server – OEM
  - Windows Vista Home Basic N
  - Windows Vista Pro Standard N
- http://www.winsupersite.com/showcase/winvista_editions.asp

Dernières vulnérabilités
Infos Microsoft (2/2)

- **Sortie de Office 2003 SP2**
  - **Date : 06 / 10 / 2005**
  - **Site : http://www.microsoft.com/downloads/details.aspx?FamilyID=57e27a97-2db6-4654-9db6-ec7d5b4dd867&DisplayLang=en**
- **Autres sorties**
  - **Vista Beta 2**
  - **IE 7 Beta 1 for XP SP2**
    - **http://www.packetstormsecurity.org/hitb05/Keynote-Tony-Chor-IE-Security-Past-Present-and-Future.ppt**
- **VirtualWifi : connexions multiples sur la même carte WiFi**
  - **http://research.microsoft.com/netres/projects/virtualwifi/**
- **Microsoft porte plainte contre 13 campagnes de spam utilisant des réseaux de zombies**
  - **http://news.zdnet.com/2100-1009_22-5917817.html**
  - **Spam capturé depuis Hotmail**

Dernières vulnérabilités
Autres avis (1/3)

- Premier "hit" pour le "Zero Day Initiative"
  - ZDI-05-001: VERITAS NetBackup Remote Code Execution
  - http://www.zerodayinitiative.com/advisories/ZDI-05-001.html
- Skype Security Evaluation
  - http://www.skype.com/security/files/2005-031%20security%20evaluation.pdf
  - Tom Berson / Anagram Laboratories
- Des outils de sécurité à surveiller
  - WehnTrust : GRSecurity pour Windows
    - http://www.wehnus.com/index.pl
  - Core Force : Mandatory Access Control pour Windows
    - http://force.coresecurity.com/
- Gartner déconseille la migration vers Office 12 avant 2008
  - http://www.generation-nt.com/actualites/9259/Migration-deconseillee-vers-Office-12
  - L'urgence est de renouveler le parc Windows
  - Note : Office 12 devra désormais être activé en ligne

Dernières vulnérabilités
Autres avis (2/3)

- La comédie musicale "Nerds" a joué à guichets fermés
  - Il est possible d'écouter les titres "Windows Rap" et "I'm Just A Nerd" en MP3
  - http://01informatique.blog.01net.com/blog/2005/10/yo_le_rap_de_bi.html
- Sony a une conception particulière de la DRM
  - http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html
- Activité virale
  - Propagation du ver Mocbot
    - Exploite la faille MS05-039 (PnP)
  - Forte activité Mytob.*
    - Reçu(s) 50 fois ce mois-ci sur la boite de l'OSSIR
  - Contournement antivirus
    - http://www.securityelf.org/magicbyte.html
    - Les antivirus se basent sur l'entête du fichier
      - Un fichier .BAT commençant par "MZ" est scanné comme un binaire
      - Il est possible de créer un fichier avec 3 points d'entrée différents selon son extension ! (.EXE, .HTML, .EML)

Dernières vulnérabilités
Autres avis (3/3)

- Michael Lynn embauché par Juniper
  - http://www.networkworld.com/news/2005/110405-juniper-cisco-hacker.html
- Symantec attaque Microsoft devant la commission européenne
  - Abus de position dominante
  - Suite aux annonces de Microsoft
    - Futur "Microsoft Client Protection"
      - Anti-virus, anti-spyware, anti-rootkit
      - http://www.lesnouvelles.net/articles/produits/748-microsoft-client-protection.html
    - Nouvelle version Antigen pour Exchange
  - Espère sans doute faire mieux que RealNetworks
    - Accord amiable de 761 million de dollars
    - Procès Rhapsody vs. MSN Search
    - Procès RealPlayer vs. Media Player

Questions / réponses

- Questions / réponses
- Date de la prochaine réunion
  - Lundi 12 décembre 2005
- N'hésitez pas à proposer des sujets et des salles