OSSIR
Groupe Sécurité Windows

Réunion du 11 juillet 2005

Revue des dernières vulnérabilités Microsoft

Nicolas RUFF

nicolas.ruff@eads.net

Dernières vulnérabilités
Avis Microsoft (1/9)

- (Avis de sécurité Microsoft depuis le 13 juin 2005)

- Juin 2005
- Bulletins "critiques"
  - MS05-025 Patch cumulatif pour IE
    - Affecte : versions de IE livrées avec
      - Windows 2000 SP3/SP4
      - Windows XP SP1/SP2
      - Windows 2003 SP0
    - Exploit :
      - "Buffer overflow" dans les images PNG
      - "Cross XML scripting" (?)
    - Crédit :
      - Mark Dowd (ISS X-Force)
      - Mark Litchfield (NGS)
      - Thor Larholm (PivX)
      - UK NISCC
    - Provoque une régression dans le support WebDAV

Dernières vulnérabilités
Avis Microsoft (2/9)

- MS05-026 Exécution de code via l'aide HTML (fichiers .CHM)
  - Affecte : lecteur d'aide HTML livré avec
    - Windows 2000 SP3/SP4
    - Windows XP SP1/SP2
    - Windows 2003 SP0
  - Exploit : "Heap Overflow" exploitable (x3) y compris sous XP SP2
  - Crédit : Peter Winter-Smith (NGS) + eEye

- MS05-027 Vulnérabilité SMB
  - Affecte :
    - Windows 2000 SP3/SP4
    - Windows XP SP1/SP2
    - Windows 2003 SP0
  - Exploit : exécution de code en mode noyau via une réponse SMB malformée
  - Crédit : Qualys

Dernières vulnérabilités
Avis Microsoft (3/9)

- **Bulletins "importants"**
  - **MS05-028 Vulnérabilité dans le service "Web Client"**
    - **Affecte :**
      - **Windows XP SP1**
      - **Windows 2003**
    - **Exploit : exécution de code sous le compte SYSTEM via une réponse WebDAV malformée**
    - **Crédit : Mark Litchfield (NGS)**
  - **MS05-029 Cross-site scripting dans OWA 5.5**
    - **Affecte : OWA (Exchange 5.5 SP4)**
    - **Exploit : cross-site scripting**
      - **<IMG SRC="jav&#X41sc
ript:alert('XSS')">**
    - **Crédit : Gaël Delalleau + iDefense**

Dernières vulnérabilités
Avis Microsoft (4/9)

- **MS05-030 Patch cumulatif pour Outlook Express**
  - **Affecte : Outlook Express livré avec**
    - **Windows 2000 SP3/SP4**
    - **Windows XP SP1/SP2**
    - **Windows 2003 SP0**
  - **Exploit : "buffer overflow" dans le client NNTP (commande LIST)**
  - **Crédit : iDefense**

- **MS05-031 Vulnérabilité dans "Microsoft Windows Interactive Training"**
  - **Affecte : Microsoft Windows Interactive Training (orun32.exe)**
  - **Exploit : "buffer overflow" dans le champ "user" des fichiers .cbo / .cbl / .cbm**
  - **Crédit : iDefense**

Dernières vulnérabilités
Avis Microsoft (5/9)

- **Bulletins "modérés"**
  - **MS05-032 Spoofing dans "Microsoft Agent"**
    - **Affecte : Microsoft Agent**
      - **Windows 2000 SP3/SP4**
      - **Windows XP SP1/SP2**
      - **Windows 2003 SP0**
    - **Exploit : Microsoft Agent peut être utilisé pour contourner les avertissements de sécurité**
    - **Crédit : Michael Krax**
  - **MS05-033 Fuite d'informations dans le client Telnet**
    - **Affecte :**
      - **Windows 2000 SP3/SP4**
      - **Windows XP SP1/SP2**
      - **Windows 2003 SP0**
      - **Windows SFU 2.2 / 3.0 / 3.5**
      - **(D'autres clients basés sur *BSD sont également affectés)**
    - **Exploit : Un serveur Telnet peut lire les variables d'environnement d'un client via la commande NEW-ENVIRON**
    - **Crédit : Gaël Delalleau + iDefense**

Dernières vulnérabilités
Avis Microsoft (6/9)

- MS05-034 Fuite d'informations dans ISA Server 2000
  - Affecte : ISA Server 2000 SP2
  - Exploit :
    - Cache Poisoning HTTP
    - Contournement des filtres via le proxy NetBIOS
  - Crédit :
    - Steve Orrin (Watchfire)
    - Han Valk

- Juillet 2005
  - 2 bulletins Windows allant jusqu'à "Critique"
  - 1 bulletin Office "Critique"
  - 1 mise à jour "non sécurité" pour Office

Dernières vulnérabilités
Avis Microsoft (7/9)

- **Révisions (nombreuses)**
  - **MS02-035 Fuite d'information lors de l'installation de SQL Server**
    - **Version 2.0 : mise à jour de l'utilitaire KillPwd**
  - **MS05-004 Vulnérabilité dans le contrôle d'accès par ASP.NET**
    - **Version 2.0 : sortie d'un patch pour Tablet PC Edition et Media Center Edition**
  - **MS05-009 Faille Messenger**
    - **Version 2.4 : correction sur la ligne de commande**
  - **MS05-019 Failles TCP/IP**
    - **Version 2.0 : nouveau patch !**
  - **MS05-025 Patch cumulatif pour IE**
    - **Version 1.1 : clarifications**
    - **Version 1.2 : régression sur le support WebDAV**
  - **MS05-026 Exécution de code via l'aide HTML**
    - **Version 1.1 : informations pour XP 64 bits**

Dernières vulnérabilités
Avis Microsoft (8/9)

- MS05-027 Vulnérabilité SMB
  - Version 1.1 : informations pour XP 64 bits
- MS05-029 Cross-site scripting dans OWA 5.5
  - Version 1.1 : correction sur la ligne de commande
- MS05-031 Vulnérabilité dans "Microsoft Windows Interactive Training"
  - Version 1.1 : mise à jour des remerciements
- MS05-032 Spoofing dans "Microsoft Agent"
  - Version 1.1 : informations pour XP 64 bits
- MS05-033 Fuite d'informations dans le client Telnet
  - Version 1.1 : mise à jour des remerciements
  - Version 1.2 : changement du risque à "modéré" pour Windows 2003

Dernières vulnérabilités
Avis Microsoft (9/9)

- **Autres avis**
  - **Spoofing de boite de dialogue via JavaScript**
    - **http://www.microsoft.com/technet/security/advisory/902333.mspx**
    - **Affecte : IE (et autres navigateurs)**
  - **"Unicode Heap Overflow" dans le composant "Java Proxy"**
    - **http://www.microsoft.com/technet/security/advisory/903144.mspx**
      - **Pas de correctif mais un outil permettant de désactiver ce composant**
    - **Affecte : javaprxy.dll (JVM Microsoft)**
      - **CLSID : 03D9F3F2-B0E3-11D2-B081-006008039BF0**
    - **Crédit : Bernhard Müller et Martin Eiszner**
  - **Sortie de Windows 2000 SP4 SRP1**
    - **Liens**
      - **Q891861**
      - **http://go.microsoft.com/fwlink/?LinkId=49772**
    - **Correctifs**
      - **Contient tous les hotfixes jusqu'au 30 avril 2005**
      - **Un changement important dans TAPI : seul les paquets RPC chiffrés sont acceptés**
      - **N'inclut pas MS03-011 (JVM) et IE 6 SP1**
    - **Rappel : il n'y aura pas de SP5 pour Windows 2000 …**

Dernières vulnérabilités
Infos Microsoft (1/1)

- **Publication du SP1 pour Windows 2003 sur Windows Update**
  - **Prévu le 26 juillet 2005**
  - **Un outil de blocage est disponible sur le site MS**
    - **http://go.microsoft.com/?linkid=3408587**
    - **Bloque jusqu'au 30 mars 2006**

- **Support WPA2**
  - **Dispo depuis le 29 avril 2005**
  - **http://support.microsoft.com/?id=893357**

- **Sortie de WSUS**
  - **Le 6 juin 2005**
  - **http://www.microsoft.com/windowsserversystem/updateservices/downloads/WSUS.mspx**

- **How A Criminal Might Infiltrate Your Network**
  - **http://www.microsoft.com/technet/technetmag/issues/2005/01/AnatomyofaHack/default.aspx**
  - **"Le jeu des 7 erreurs" ☺**

Dernières vulnérabilités
Autres avis (1/3)

- De "vraies" collisions MD5 sur des textes en anglais
  - Utilise une mise en page conditionnelle en PostScript
  - Quelques heures de calcul sur un PC standard
  - Références
    - http://www.cits.rub.de/MD5Collisions/
    - http://www.cits.rub.de/imperia/md/content/magnus/letter_of_rec.ps
    - http://www.cits.rub.de/imperia/md/content/magnus/order.ps
    - MD5 = a25f7f0b 29ee0b39 68c86073 8533a4b9

- Retour sur une "nouvelle" attaque : HTTP Request Smuggling
  - Envoi de plusieurs entêtes identiques avec des valeurs différentes
  - Ex.1
    - POST http://SITE/foobar.html HTTP/1.1
Host: SITE
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
Content-Length: 44

Dernières vulnérabilités
Autres avis (2/3)

- Ex.2
  - GET /poison.html HTTP/1.1
    Host: SITE
    Bla:
    GET http://SITE/page_to_poison.html HTTP/1.1
    Host: SITE
    Connection: Keep-Alive

- Le créateur du ver Sasser condamné
  - 21 mois de prison avec sursis
  - Peine relativement clémente compte tenu des 143 plaintes déposées

Dernières vulnérabilités
Autres avis (3/3)

- **Deux vulnérabilités Java importantes**
  - **#1**
    - **Affecte :**
      - **<= J2SE 5.0 Update 1**
    - **Exploit : exécution d'applets dans la zone de confiance via des fichiers JNLP malformés**
  - **#2**
    - **Affecte :**
      - **<= J2SE 1.4.2 Update 7**
      - **< = J2SE 5.0 Update 1**
    - **Exploit : exécution d'applets dans la zone de confiance via des appels système (non spécifiés dans l'avis)**
    - **Crédit : Adam Gowdiak**
  - **Risque d'exploitation par les auteurs de spywares important**

Questions / réponses

- **Questions / réponses**
- **Date de la prochaine réunion**
  - **Pas de réunion en août**
  - **Lundi 12 septembre 2005**
- **N'hésitez pas à proposer des sujets et des salles**