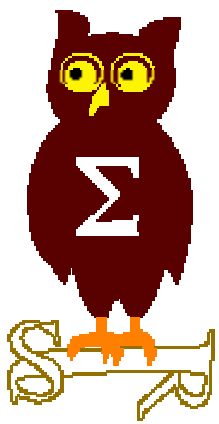
# OSSIR
# Groupe Sécurité Windows

## Réunion du 9 octobre 2006



# Revue des dernières vulnérabilités Microsoft

**Nicolas RUFF**

**EADS-CCR**

**nicolas.ruff@eads.net**

# Dernières vulnérabilités
# Avis Microsoft (1/3)

- (Avis de sécurité Microsoft depuis le 11 septembre 2006)

- Septembre 2006

  - MS06-052 Vulnérabilité dans le protocole PGM (Pragmatic General Multicast)
    - Affecte : Windows XP SP1/SP2
    - Exploit : exécution de code à distance
    - Crédit : David Warden / NuPaper

  - MS06-053 "Cross-site scripting" dans le service d'indexation
    - Affecte : Windows toutes versions supportées
      - Exploitation via Internet Explorer
    - Exploit : contournement des filtres anti-XSS par encodage UTF-7
      - http://isc.sans.org/diary.php?storyid=1760&rss
    - Crédit : Eiji James Yoshida

# Dernières vulnérabilités
# Avis Microsoft (2/3)

- **MS06-054 Exécution de code via Publisher**
  - **Affecte : Office 2000 SP3, Office XP SP3, Office 2003 SP1/SP2**
  - **Exploit : exécution de code à l'ouverture d'un ".pub"**
  - **Crédit : Stuart Pearson / Computer Terrorism**

- **MS06-055 Exécution de code via un script VML [ bulletin hors cycle ]**
  - **Affecte : Internet Explorer toutes versions supportées**
  - **Exploit : exécution de code ("buffer overflow" dans setSlice())**
  - **Crédit : ISS, iDefense, Dan Hubbard / Websense**

- **Révisions**
  - **MS06-040**
    - **Version 2.0 : problème Q921883 corrigé**
  - **MS06-042**
    - **Version 3.0 : nouveau "buffer overflow" corrigé dans les URLs longues**

# Dernières vulnérabilités
# Avis Microsoft (3/3)

- Advisories
  - Q925143 Vulnérabilité Flash Player
    - Installer Flash 9.0.16 (les versions 8 et antérieures ne sont plus supportées)
  - Q922582 Problème d'incompatibilité avec les "minifilters" réseau
    - Lien avec la sécurité => pas de WindowsUpdate ☺ (erreur 0x80070002)
  - Q925444 Vulnérabilité dans le contrôle ActiveX "DirectAnimation" (daxctle.ocx)
  - Q925568
    - Vulnérabilité dans le traitement des scripts VML (Internet Explorer – vgx.dll)
    - Utilisé en "0day" dans la nature
      - http://sunbeltblog.blogspot.com/2006/09/seen-in-wild-zero-day-exploit-being.html
    - Patch non officiel disponible chez ZERT
    - Corrigé par un bulletin "hors cycle" (MS06-055)
  - Q925944 "0day" PowerPoint
  - Q926043 Vulnérabilité dans le contrôle ActiveX "WebViewFolderIcon"
    - Disponible dans Metasploit

# Dernières vulnérabilités
# Infos Microsoft (1/2)

- **BrowserShield**
  - Réécrire les flux Web pour se protéger des attaques
  - http://research.microsoft.com/research/shield/
- **Cisco NAC et Microsoft NAP interopérables**
  - http://go.microsoft.com/?linkid=5453359
- **Le patch le plus rapide de l'univers**
  - Après le cassage du système de DRM de Windows Media, Microsoft publie un patch en 3 jours
  - Malheureusement le patch est cassé en 5 jours ☺
- **Windows Fundamentals**
  - Un "XP Light" pour le matériel ancien
  - Non disponible publiquement
  - http://www.microsoft.com/licensing/programs/sa/benefits/fundamentals.mspx
  - http://en.wikipedia.org/wiki/Windows_Fundamentals_for_Legacy_PCs

# Dernières vulnérabilités
# Infos Microsoft (2/2)

- **Beta et RC**
  - **Vista RC1 !**
  - **IE7 RC1**
  - **Microsoft Virtual Server 2005 R2 SP1 Beta 2**
  - **Media Player 11 Beta 2**
  - **.NET Framework 3.0 RC**

# Dernières vulnérabilités
# Autres avis (1/3) – failles

- Un "0day" Powerpoint en circulation
  - Intégré dans l'antivirus Microsoft le 23 septembre, soit avant la diffusion publique …
- Une faille du "browser bug of the day" serait exploitable
  - Composant affecté : webvw.dll (IE)
- Firefox 1.5.0.7 disponible
  - http://www.mozilla.org/projects/security/known-vulnerabilities.html#firefox1.5.0.7
- Falsification des signatures RSA 1.5
  - http://www.securityfocus.com/bid/19849
  - Affecte : Windows 2000 < SP4, OpenSSL < 0.9.7k, OpenSSL < 0.9.8c, …
  - Liste des autorités de certification utilisant un module RSA égal à 3
    - http://www.cdc.informatik.tu-darmstadt.de/securebrowser/
    - Ex. Entrust

# Dernières vulnérabilités
# Autres avis (2/3) – virus et spywares

- Quelques nouveaux virus innovants
  - PWS-Satiloler
    - Désactive WFP
  - Un autre virus …
    - Se protège contre la détection grâce à EFS
    - Communique avec son maître via un canal caché (images GIF)
    - http://www.avertlabs.com/research/blog/?p=77
  - J2ME/Redbrowser, J2ME/Wesber
    - Envoient des SMS surtaxés (jusqu'à $15/message)
  - Botnet "Opanki"
    - Utilise Google Analytics pour répartir géographiquement son réseau
  - Un ver se propage sur MSN Messenger
    - http://isc.sans.org/diary.php?storyid=1730
    - Les ".pif" sont bloqués par MSN … mais pas les ".PIF" !
- SMSing : le phishing par SMS
  - http://www.avertlabs.com/research/blog/?p=74

# Dernières vulnérabilités
# Autres avis (3/3)

- ZeroDay Emergency Response Team (ZERT)
  - http://isotf.org/zert/
- "Backdoors" dans les formats de fichier populaires
  - PDF
    - http://michaeldaw.org/md-hacks/backdooring-pdf-files
    - Supporte JavaScript et ADBC
  - MOV (Quicktime)
    - http://www.gnucitizen.org/blog/backdooring-quicktime-movies/
    - Supporte également JavaScript

# Questions / réponses

- **Questions / réponses**
- **Date de la prochaine réunion**
  - **Prochaine réunion le 13 novembre 2006**
- **N'hésitez pas à proposer des sujets et des salles**