

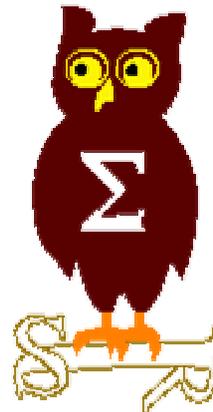


EdelWeb

# OSSIR

## Groupe Sécurité Windows

Réunion du 12 janvier 2004





**EdelWeb**

# **Revue des dernières vulnérabilités Windows**

**Nicolas RUFF**

**nicolas.ruff@edelweb.fr**

# Dernières vulnérabilités

## Avis Microsoft (1/1)



EdelWeb

- **Avis de sécurité Microsoft depuis le 08/12/2003**
  - Pas de bulletin en décembre !
  
- **Mise à jour de l'add-on WPA**
  - Q826942
    - [http://support.microsoft.com/default.aspx?scid=kb;\[LN\];826942](http://support.microsoft.com/default.aspx?scid=kb;[LN];826942)
  - **Nombreux bugfixes**
    - Erreurs lors de l'utilisation conjointe TKIP / AES
    - Réponses RC4 incorrectes
    - Etc.

# Dernières vulnérabilités Infos Microsoft (1/2)



EdelWeb

- **"Réseaux WiFi sécurisés avec Windows XP et 2003"**
  - <http://go.microsoft.com/?linkid=344332>
  
- **"Security Readiness Kit"**
  - <http://www.microsoftsecuritysolutions.com/Default.asp?id=sec>
  
- **Microsoft envisage de distribuer des CDs de mise à jour pour les gens sans accès Internet**
  
- **Processus de transition suite à l'arrêt de MS JVM**
  - <http://www.microsoft.com/france/infos/java/default.asp>



## ■ Plus d'informations sur XP SP2

- Firewall :  
<http://www.microsoft.com/downloads/details.aspx?FamilyID=4454e0e1-61fa-447a-bdcd-499f73a637d1&DisplayLang=en>
- Global :  
[http://download.microsoft.com/download/8/7/9/879a7b46-5ddb-4a82-b64d-64e791b3c9ae/WinXPSP2\\_Documentation.doc](http://download.microsoft.com/download/8/7/9/879a7b46-5ddb-4a82-b64d-64e791b3c9ae/WinXPSP2_Documentation.doc)

## ■ Microsoft avait "oublié" de publier le patch FrontPage sur WindowsUpdate

- Sorti en décembre, un mois après le bulletin
- Patch "critique" pour les systèmes avec FrontPage installé



### ■ Masquage d'URLs dans IE

- Affecte : au moins IE 6 et 6 SP1
- Exploit : `http://www.microsoft.com%01@fake.com`
- Pas de patches officiels => développement sauvage de patches "open source" et/ou payants
  - Le patch "Openwares" provoque un BoF dans IE !

### ■ Document CoreLabs "DCE/RPC New Attack Vectors"

- Le ver Blaster aurait pu être bien pire
  - Des services RPC écoutent sur des ports non privilégiés
    - Ex. Workstation TCP/1025
  - Des services RPC répondent aux messages en "broadcast"
  - Le flag "idempotent" (RPCv4) permet d'éviter la phase de négociation, et donc de spoofer l'adresse source

# Dernières vulnérabilités

## Autres avis (2/3)



EdelWeb

### ■ Exécution de code dans IE

- Affecte : IE 5.01, 5.5, 6.0
- Exploit :
  - Il est possible de lancer un fichier CHM déjà présent sur le disque dur
  - Il faut donc être capable de télécharger un fichier à un emplacement connu du disque
  - Nouvelle idée : utiliser les répertoires temporaires des plugins (ex. Winamp)
- <http://www.securityfocus.org/bid/9320>
- Pas de patch disponible

### ■ Bypass de la protection des formulaires Word

- Affecte : Word 97 - 2003
- Exploit :
  - remplacer "<w:UnprotectPassword>ABCDEF01</w:UnprotectPassword>"
  - par "00000000"
- <http://support.microsoft.com/?id=822924>



### ■ Protection proactive d'IE

- Qwik-Fix par PivX

- Anciennement site de failles IE non patchées

- Aujourd'hui outil gratuit Qwik-Fix

- <http://www.pivx.com/qwikfix/index.html>

- Post de Thor Larholm :

- <http://www.ntbugtraq.com/default.asp?pid=36&sid=1&A2=ind0312&L=ntbugtraq&P=396>

### ■ Bug IIS 5.0

- Affecte : IIS 5.0 (IIS 6.0 n'est pas affecté)

- Exploit : le verbe HTTP "TRACK" est traité comme "TRACE", mais sans journalisation



- Questions / réponses
  
- Date de la prochaine réunion :
  - Lundi 9 février 2004
  
- N'hésitez pas à proposer des sujets et des salles