

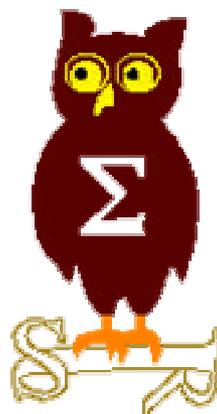


EdelWeb

# OSSIR

## Groupe Sécurité Windows

Réunion du 3 novembre 2003





---

**EdelWeb**

# **Revue des dernières vulnérabilités Windows**

**Nicolas RUFF**  
**nicolas.ruff@edelweb.fr**

# Dernières vulnérabilités

## Avis Microsoft (1/3)



EdelWeb

- **Avis de sécurité Microsoft depuis le 06/10/2003**
  - **MS03-041 : Vulnerability in Authenticode Verification Could Allow Remote Code Execution (823182)**
    - Affecte : Windows NT4, 2000, XP, 2003
    - Exploit : ?
  
  - **MS03-042 : Buffer Overflow in Windows Troubleshooter ActiveX Control Could Allow Code Execution (826232)**
    - Affecte : Windows 2000 (Tshoot.ocx) + ?
    - Exploit :
      - `<object id="test" classid="CLSID:4B106874-DD36-11D0-8B44-00A024DD9EFF" >`  
`</object> <script> test.RunQuery2("longstringhere", "", ""); </script>`
  
  - **MS03-043 : Buffer Overrun in Messenger Service Could Allow Code Execution (828035)**
    - Affecte : Windows NT4, 2000, XP, 2003
    - Exploit : permet d'obtenir les droits SYSTEM à distance sans authentification sur un service démarré par défaut ...
    - Microsoft prétendait que le service était sans danger malgré le spam 😊
      - [http://www.usatoday.com/tech/news/2003-09-24-popups\\_x.htm](http://www.usatoday.com/tech/news/2003-09-24-popups_x.htm)

# Dernières vulnérabilités

## Avis Microsoft (2/3)



EdelWeb

- **MS03-044 : Buffer Overrun in Windows Help and Support Center Could Lead to System Compromise (825119)**
  - **Affecte :**
    - Windows XP, 2003
    - NT4, 2000, ME bien que la fonction ne soit pas accessible par hcp://
  - **Exploit :**
    - <http://www.ngssoftware.com/advisories/ms-pchealth.txt>
  
- **MS03-045 : Buffer Overrun in the ListBox and in the ComboBox Control Could Allow Code Execution (824141)**
  - **Affecte :** Windows NT4, 2000, XP, 2003 (user32.dll)
  - **Exploit :**
    - Messages CD\_DIR et LB\_DIR avec un nom de fichier très long provoque un "overflow" dans UTILMAN
    - Permet de devenir SYSTEM

# Dernières vulnérabilités

## Avis Microsoft (3/3)



EdelWeb

- **MS03-046 : Vulnerability in Exchange Server Could Allow Arbitrary Code Execution (829436)**
  - Affecte : Exchange 5.5 et 2000
  - Exploit :
    - Exchange 5.5 : DoS via SMTP
    - Exchange 2000 : exécution de code à distance dans le contexte SYSTEM via SMTP
- **MS03-047 : Vulnerability in Exchange Server 5.5 Outlook Web Access Could Allow Cross-Site Scripting Attack (828489)**
  - Affecte : Exchange 5.5 OWA
  - Exploit : cross-site scripting (XSS)
- **Faille Windows Media**
  - Exécution de commandes dans la zone locale via DHTML
  - Non patchée par MS03-040

# Dernières vulnérabilités

## Avis Microsoft (re-releases)



EdelWeb

- MS03-045
- MS03-047
  - Patches présentant des incompatibilités avec des logiciels tiers
- MS03-042
- MS03-043
- MS03-045
  - Incompatibilité avec les débogueurs

# Dernières vulnérabilités Infos Microsoft (1/1)



EdelWeb

- **Windows XP Media Center**
  - Un PC – TV – magnétoscope – etc.
- **Sortie du SRP1 pour XP**
  - 22 correctifs post-SP1
  - <http://support.microsoft.com/?kbid=826939>
  - N'inclut pas les correctifs (critiques) MS03-041 et ultérieurs ...
- **SMS Sender pour Windows XP**
  - <http://www.microsoft.com/downloads/details.aspx?FamilyId=06A4F997-7F69-4891-8929-37B9041924A2&displaylang=fr>
- **ISA Server 2000 certifié EAL 2**
  - <http://www.microsoft.com/france/windowsserversystem/info/info.asp?mar=/france/isaserver/info/20030925-commoncriteria.html>
- **Fin du support JVM Microsoft repoussé au 30 septembre 2004**

# Dernières vulnérabilités

## Autres avis (1/1)



EdelWeb

### ■ Vulnérabilité "shell folders"

- Affecte : Windows 2003 (+ autres versions ?)
- Exploit :
  - `<a href="shell:cache\..\..\Local Settings\Temp\exploit.html">Exploit</a>`

### ■ Vulnérabilité Hotmail

- Il suffit de préfixer les tags avec 3+ tirets pour outrepasser les filtres HTML
- Exploit :
  - `---<LINK, ---<object, ---<iframe`

### ■ Comment déprotéger un PowerPoint contre la modification

- Ouvrir le document en lecture seule
- Lancer l'éditeur de scripts
- Une copie non protégée du fichier PowerPoint est placée dans le répertoire `<temp>\MSE\<nom de fichier>`



- Questions / réponses
  
- Date de la prochaine réunion :
  - Lundi 8 décembre 2003
  
- N'hésitez pas à proposer des sujets et des salles