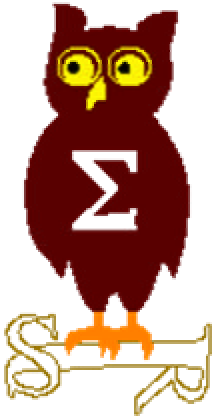
EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 13 mai 2002



EdelWeb

Revue des dernières vulnérabilités de Windows 2000

Nicolas RUFF

nicolas.ruff@edelweb.fr

Dernières vulnérabilités (1/5)

EdelWeb

- **Avis de sécurité Microsoft depuis le 11/03/2002 :**
  - **MS02-014 : débordement de buffer dans le GUI Windows**
    - **Si un handler d'extension « xxx:// » a été désinstallé**
  - **MS02-015 : patch cumulatif pour IE**
    - **Exécution des scripts inclus dans un cookie dans la zone locale**
    - **Exécution de commandes sur le poste de travail connu sous le nom de « simplebind »**

```
<span datasrc="#oExec" datafld="exploit" dataformatas="html"></span>
<xml id="oExec">
<![CDATA[
<object id="oFile" classid="clsid:11111111-1111-1111-1111-111111111111"
codebase="c:/winnt/system32/calc.exe"></object>
]]></xml>
```

  - **MS02-016 : patch disponible pour la vulnérabilité « verrouillage des stratégies de groupe » (documentée depuis plusieurs mois)**
  - **MS02-017 : débordement de buffer dans le parser de chemins UNC**
    - **Exploit SYSTEM local uniquement**

Dernières vulnérabilités (2/5)

- **MS02-018 : patch cumulatif pour 10 nouvelles vulnérabilités IIS 4.0, 5.0 et 5.1**
  - **Nombreux exploits SYSTEM distants possibles**
  - **5 débordements de tampon (buffer overrun)**
  - **2 failles de type DoS (Denial of Service)**
  - **3 vulnérabilités de type CSS (Cross-Site Scripting)**
- **MS02-019**
  - **Vulnérabilités dans de nombreux produits Microsoft sur MacOS 8, 9, X**
  - **http://www.w00w00.org/**
- **MS02-020**
  - **« Buffer overflow » dans de nombreuses procédures étendues (xp_???)**
  - **Affecte SQL Server 7.0 et 2000**
  - **Problème connu depuis plus d'un mois**
- **MS02-021**
  - **Lorsque Word est utilisé comme éditeur de mail avec Outlook 2000 et XP, les paramètres de sécurité de la zone Internet ne sont appliqués**

Dernières vulnérabilités (3/5)

- MS02-022
  - Débordement de buffer dans le contrôle ActiveX MSN Messenger Chat

```
<object classid="clsid:9088E688-063A-4806-A3DB-6522712FC061" width="455" height="523">
<param name="_cx" value="12039">
<param name="_cy" value="13838">
<param name="BackColor" value="50331647">
<param name="ForeColor" value="43594547">
<param name="RedirectURL" value="">
<param name="ResDLL" value="AAAAAAA[27,257 bytes is where the EIP starts]">
</object>
```

- Q320751
  - Déni de service sur le port TCP/445 (dans le service LANMAN)

■ Mises à jour
- MS02-006 version 6
  - Vulnérabilités SNMP multiples
  - Problème de stabilité des patches
- MS02-013 version 2
  - Exécution de code en dehors de la « sandbox » Java

Dernières vulnérabilités (4/5)

EdelWeb

- **Windows XP**
  - **Si un utilisateur change son mot de passe avant que le système lui demande, la stratégie de comparaison avec les N mots de passe précédents n'est pas appliquée**
  - **Bien que Windows XP limite l'accès réseau aux comptes sans mot de passe, ceci n'affecte pas le compte « invité » (s'il est activé)**
  - **Exploit « DebPloit »**
    - **Permet d'émettre des commandes de déboguage par une connexion directe au Session Manager SubSystem (SMSS)**
- **Office XP**
  - **Outrepassement de la restriction sur les pièces jointes dans Outlook XP**
  - **Advisory Guninski #53**

Dernières vulnérabilités (5/5)

- **Internet Explorer**
  - **Il est possible de tester l'existence de fichiers à l'aide de la propriété «complete»**
    - **http://spoor12.edup.tudelft.nl/skylined**
  - **Cross-site scripting**
    - **Affecte le contrôle WebBrowser**
    - **http://jscript.dk/adv/TL002/**
- **Autres**
  - **Débordement de buffer dans le contrôle ActiveX Flash Player 6.0**
  - **Nouvelle variante dans le débordement de buffer affectant AOL Instant Messenger**

Questions / réponses

EdelWeb

- **Questions / réponses**

- **Date des prochaines réunions :**
  - **Lundi 10 juin 2002**
  - **Lundi 8 juillet 2002**