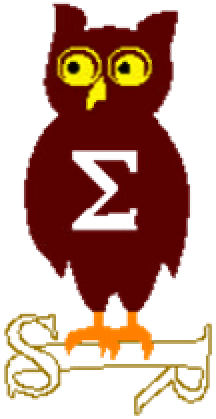
EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 07 octobre 2002



EdelWeb

Revue des dernières vulnérabilités Windows

Nicolas RUFF

nicolas.ruff@edelweb.fr

Dernières vulnérabilités
Avis Microsoft (1/2)

- **Avis de sécurité Microsoft depuis le 09/09/2002**
  - **MS02-051**
    - **Encrypted RDP Packet Information Leakage Vulnerability**
      - **http://online.securityfocus.com/bid/5711**
    - **RDP Keystroke Injection Vulnerability**
      - **http://online.securityfocus.com/bid/5712**
  - **MS02-052**
    - **Corrige 3 vulnérabilités JVM**
    - **Permettent l'exécution de code hors de la « sandbox » via JDBC**
    - **Il y aurait une dizaine de failles à corriger en tout !**
  - **MS02-053**
    - **Vulnérabilité FPSE 2000 (DoS uniquement) et 2002 (« buffer overflow »)**
  - **MS02-054**
    - **2 vulnérabilités dans la fonction « ZIP Folders »**
    - **« Buffer overflow » exploitable lors de l'ouverture d'une archive**
    - **Extraction de fichiers vers un chemin « en dur »**
    - **Affecte Windows 98 Plus!, ME, XP**

Dernières vulnérabilités
Avis Microsoft (2/2)

- MS02-055
  - « Buffer overflow » dans le contrôle ActiveX d'affichage de l'aide
  - Exécution de code par le biais d'un lien dans un fichier .CHM
    - Les fichiers .CHM provenant d'Internet sont exécutés dans la Local Computer Zone
  - Affecte toutes les versions de Windows (98, ME, NT4, 2000, XP)
- MS02-056
  - Patch cumulatif pour SQL Server 7.0/2000 et MSDE 1.0/2000
  - 3 nouvelles vulnérabilités
  - « Buffer overrun » dans la phase d'authentification (SQL/MSDE 2000) [Exploitable]
  - « Buffer overrun » dans la console DBCC (SQL 7.0/2000) [Exploitable localement vers SYSTEM]
  - Écriture de fichiers avec les privilèges SQL Agent par le biais des tâches planifiées (SQL 7.0/2000)
- MS02-057
  - 3 vulnérabilités dans « Services for Unix 3.0 »
  - « Integer overflow » dans la librairie XDR pour Sun [exploitable]
  - « Buffer overrun » dans les appels RPC [DoS]
  - Erreur d'implémentation dans la librairie Sun RPC [DoS]
  - Toutes les applications créées avec Interix Sun RPC SDK doivent être recompilées

Dernières vulnérabilités
Vulnérabilités corrigées silencieusement (1/1)

- **Débordement de buffer dans un contrôle ActiveX**
  - **Contrôle DirectX XWEB.OCX**
  - **Corrigé dans 2000 SP3 et XP SP1**
- **Vulnérabilité « hard links »**
  - **Si un lien physique est créé puis détruit, les opérations effectuées au travers de ce lien ne sont pas traçables dans le journal d'audit**
  - **Corrigé dans 2000 SP3**
- **Destruction de n'importe quel fichier via IE**
  - **hcp://system/DFS/uplddrvinfo.htm?file://c:\test***
  - **Faille due à Remote Assistance**
  - **Corrigé dans XP SP1**
- **Déni de service Remote Desktop**
  - **http://online.securityfocus.com/bid/5713**
  - **Affecte XP et .Net mais pas 2000**
  - **Corrigé silencieusement dans XP SP1**

Dernières vulnérabilités
Autres avis (1/1)

- Vulnérabilités multiples dans la JVM Microsoft
  - http://www.solutions.fi/index.cgi/news_2002_09_09?lang=eng
- Le mode « révision » de Word permet de voler n'importe quel fichier
  - http://www.woodyswatch.com/office/archtemplate.asp?v7-n42
  - http://www.woodyswatch.com/office/archtemplate.asp?v7-n43
- Faille « SMTP Mail Reassembly »
  - Extension normative supportée par Outlook Express
  - Passe les filtres de contenu SMTP
  - http://www.securiteam.com/securitynews/5YP0A0K8CM.html
- Pas de vérification des permissions d'exécution sur les applications 16 bits
  - Command /c 16bitapp.exe
- Déni de service (exploitable ?)
  - Affecte Windows 2000/XP
  - Port 1723
  - « Buffer overflow » dans la préauthentification
  - http://www.phion.com/adv/index.html

Autres informations

EdelWeb

- Alliance Intel – Verisign pour intégrer un certificat dans chaque processeur
- Disponibilité du SP1 pour Windows XP (anglais et français)
  - Ne s'installe pas sur des Windows XP « pirates »
    - 2 numéros de série « blacklistés »
    - Un contournement est déjà disponible

Questions / réponses

EdelWeb

- **Questions / réponses**

- **Date de la prochaine réunion :**
  - **Lundi 4 novembre 2002**