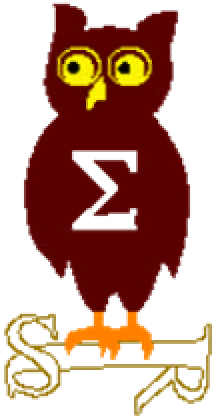
EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 9 décembre 2002



EdelWeb

Revue des dernières vulnérabilités Windows

Nicolas RUFF

nicolas.ruff@edelweb.fr

Dernières vulnérabilités
Avis Microsoft (1/5)

- **Avis de sécurité Microsoft depuis le 07/10/2002**
  - **MS02-058 : débordement de buffer dans l'affichage d'une erreur S/MIME**
    - **Affecte Outlook Express 5.5 (sauf SP2) et 6.0 (sauf SP1)**
    - **Exploitable en déni de service ou exécution de code**
  - **MS02-059 : vol d'information par le biais des champs de fusion**
    - **Affecte Word et Excel**
    - **Des fichiers peut être inclus silencieusement lors de l'ouverture d'un document**
    - **L'information ne peut être exploitée que si le document est ensuite transmis**
    - **Le patch ne protège que « partiellement » Word 97 (!)**
  - **MS02-060 : destruction de fichier par le biais d'un lien Remote Assistance**
    - **Affecte Windows XP**
    - **Déjà présentée lors de la dernière réunion (hcp://…)**
    - **Corrigé dans le SP1**

Dernières vulnérabilités
Avis Microsoft (2/5)

- **MS02-061 : élévation de privilèges par les tâches Web**
  - Affecte SQL Server 7.0 et 2000
  - N'importe quel utilisateur peut modifier les tâches Web de n'importe quel autre
  - Il est possible de créer des tâches dans le contexte SYSTEM
- **MS02-062 : patch cumulatif pour IIS**
  - Concerne IIS 4.0, 5.0 et 5.1
  - 4 vulnérabilités :
    - Élévation de privilège locale par les filtres ISAPI (IWAM -> SYSTEM)
    - Déni de service système par requête WebDAV malformée
    - Upload et exécution de fichiers .COM possible par WebDAV avec uniquement des droits en écriture sur un répertoire
    - Cross-site scripting
- **MS02-063 : vulnérabilité PPTP**
  - Affecte RRAS dans Windows 2000 / XP (+ autres versions de Windows où PPTP a été installé comme composant optionnel)
  - Déni de service système
  - Exploitabilité douteuse
  - (Vulnérabilité déjà mentionnée lors de la dernière réunion)

Dernières vulnérabilités
Avis Microsoft (3/5)

- **MS02-064 : permissions par défaut laxistes**
  - **Affecte Windows 2000**
  - **La permission « contrôle total » accordées par défaut sur la racine du disque système permet l'implantation de Chevaux de Troie**
  - **Ces Chevaux de Troie sont activés par « Démarrer / exécuter », un script de logon, un logon Telnet, etc.**
  - **(Vulnérabilité connue depuis longtemps …)**
- **MS02-065 : « buffer overflow » dans MDAC**
  - **Un paquet HTTP malformé permet d'exécuter du code**
  - **Fonctionne côté client ou côté serveur !**
  - **Côté serveur : affecte MDAC 2.1, 2.5, 2.6 Remote Data Service**
  - **Côté client : affecte IE 5.01, IE 5.5, IE 6.0**
- **MS02-066 : patch cumulatif pour IE**
  - **Concerne IE 5.01, IE 5.5 et IE 6.0**
  - **« Buffer overflow » lors de la lecture de fichiers PNG**
  - **Redirection transparente par des caractères spéciaux dans une URL encodée**
  - **Lecture / écriture de fichiers locaux (le tag OBJECT permet de déterminer l'emplacement du répertoire Temporary Internet Files)**
  - **Lecture / exécution de fichiers locaux (x3)**

Dernières vulnérabilités
Avis Microsoft (4/5)

- **MS02-067 : déni de service Outlook**
  - **Affecte Outlook 2002**
  - **Un entête malformé permet de bloquer complètement le logiciel**
- **MS02-068 : patch cumulatif pour IE**
  - **Concerne IE 5.5 et 6.0**
  - **Elimine une nouvelle vulnérabilité de divulgation d'informations inter-domaines**
  - **Niveau de sévérité réévalué de « medium » à « high » suite à un article dans BugTraq**

Dernières vulnérabilités
Avis Microsoft (5/5)

- **Bulletins mis à jour depuis le 07/10/2002**
  - **MS02-050 v2 : gestion de la chaîne de confiance de certificats erronée**
    - **Affecte Windows / IE / Office / Outlook**
    - **Re-release du patch**
    - **Erreur lors de la vérification de signatures sur les drivers**
    - **Supprime une variante de la vulnérabilité initiale**

- **Autres infos Microsoft**
  - **Office XP SP3 (anglais uniquement)**

Dernières vulnérabilités
Autres avis (1/1)

- **Authentification SA faible**
  - 1 : le mot de passe est converti en Unicode
  - 2 : les 4 MSB sont échangés avec les 4 LSB dans chaque octet
  - 3 : XOR avec 0xA5
- **Exploit D-Day**
  - Affecte IE toutes versions sauf SP1
  - Cross-frame scripting grâce à la propriété « Document » (distincte de « document »)
- **Déni de service RPC**
  - Affecte Windows 2000 SP3, Windows XP SP1
  - Un pointeur NULL dans une commande RPC arrête le service
  - http://www.immunitysec.com/vulnerabilities/
- **9 vulnérabilités IE (patché dans MS02-068 ?)**
  - http://sec.greymagic.com/adv/gm012-ie/
  - Permettent de récupérer le nom du répertoire cache
  - Internet Explorer v5.5 SP2 et 6.0 sont totalement vulnérables
  - Internet Explorer v5 SP 2 est totalement immunisé
  - Internet Explorer v6.0 SP1 est immunisé contre 8 de ces 9 vulnérabilités

News Microsoft (1/2)

EdelWeb

- KerbSniff / KerbCrack
  - « Brute force » sur la phase de pré-authentification
  - Outil publié (sans code source)
  - Vulnérabilité déjà connue depuis plusieurs mois
- Mise à jour de l'aide Windows XP sur la sécurité
  - http://www.microsoft.com/france/windows/xp/securite/default.asp
  - Recommandations
    - Appliquer les correctifs Windows et Office
    - Utiliser un antivirus à jour
    - Utiliser un mot de passe robuste et changé régulièrement
    - Utiliser le firewall intégré
  - Recommandations avancées
    - Formater en NTFS
    - Utiliser WindowsUpdate
    - Utiliser EFS
    - Utiliser le scanneur de vulnérabilités en ligne
    - Mettre en œuvre une stratégies de sécurité locale

News Microsoft (2/2)

EdelWeb

- **Hotline Sécurité Virus Microsoft**
  - **0825 827 829**
  - **0,15 € / minute**
- **Campagne « Enjeu Sécurité »**
  - **http://www.microsoft.com/france/partenaires/campagne-enjeux_securite/default.asp**
  - **Objectif : migrer les PME vers Office XP, Windows XP et Windows 2000 Server …**
- **Windows 2000 est certifié EAL 4 + ALC FLR 3 (Systematic Flaw Remediation)**
  - **3 guides de configuration : utilisateur, administrateur, sécurité**
    - **http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/issues/W2kCCUG/default.asp**
    - **http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/issues/W2kCCAdm/default.asp**

Questions / réponses

EdelWeb

- **Questions / réponses**

- **Date de la prochaine réunion :**
  - **Lundi 13 janvier 2003**