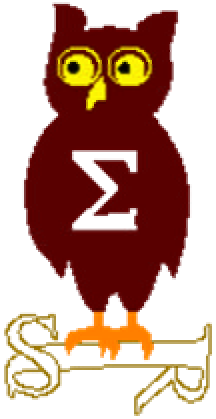
EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 09 septembre 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 08/07/2002**
  - **MS02-032 v2**
    - **Affecte Windows Media Player 6.4, 7.1 et XP**
    - **Nouveau patch cumulatif (l'ancien ne l'était pas vraiment)**
  - **MS02-034**
    - **Affecte SQL Server 2000 et MSDE 2000**
    - **2 vulnérabilités en « buffer overflow » permettant d'obtenir les droits du service SQL (potentiellement SYSTEM)**
    - **Stockage non sûr du mot de passe du compte de service SQL (potentiellement SYSTEM)**
  - **MS02-035**
    - **Affecte SQL Server 7.0, SQL Server 2000 et MSDE 1.0**
    - **Permet de retrouver le mot de passe SA dans un fichier de configuration (SETUP.ISS)**
  - **MS02-036**
    - **Affecte Microsoft Metadirectory Service 2.2**
    - **Accès / modification d'informations de configuration sans authentification**

Dernières vulnérabilités
Avis Microsoft (2/5)

- **MS02-037**
  - **Affecte Microsoft Exchange 5.5**
  - **« Buffer overflow » permettant l'exécution de code dans le contexte SYSTEM**
  - **Le « payload » est envoyé dans la réponse à une requête DNS inverse suite à une commande EHLO émise par IMC (Internet Mail Connector)**
- **MS02-038**
  - **Affecte SQL Server 2000, MSDE 2000**
  - **« Buffer overflow » dans les outils de contrôle de cohérence permettant d'acquérir les droits SYSTEM (exploitable par sysadmin et db_owner)**
  - **Exécution de commandes sur le système par le biais de procédures stockées (exploitable par db_owner et tout utilisateur interactif)**
- **MS02-039**
  - **Affecte SQL Server 2000**
  - **2 vulnérabilités en « buffer overflow » permettant l'exécution de code dans le contexte SYSTEM**
  - **1 déni de service par tempête de paquets entre deux installations de SQL Server**
  - **Basés sur des défaillances du service de résolution (UDP/1434)**

Dernières vulnérabilités
Avis Microsoft (3/5)

- MS02-040
  - Affecte le composant MDAC
  - « Buffer overflow » dans plusieurs fonctions d'accès à une base SQL
- MS02-041
  - Vulnérabilités multiples dans Content Management Server
    - « Buffer overflow » dans le contexte du service CMS
    - « Upload » de fichiers sur le serveur
    - Injection SQL
- MS02-042
  - Vulnérabilité dans Network Connexion Manager
  - Permet à un utilisateur interactif d'obtenir les droits SYSTEM
  - Affecte Windows 2000
- MS02-043
  - Patch cumulatif pour SQL Server 7.0 et 2000
  - Corrige une vulnérabilité supplémentaire permettant l'exécution de procédures stockées par un utilisateur non privilégié

Dernières vulnérabilités
Avis Microsoft (4/5)

- MS02-044
  - 3 vulnérabilités dans Office Web Components
    - Host() permet d'exécuter n'importe quelle commande
    - LoadText() permet de lire n'importe quel fichier
    - Copy()/Paste() permet de lire le presse-papiers
  - Affecte Office 2000, Office XP, BackOffice Server, BizTalk Server, Commerce Server, ISA Server, Money, Project, Small Business Server
- MS02-045
  - Déni de service par envoi de paquet SMB malformé (SMB_COM_TRANSACTION)
  - Possibilité d'exécution de code : inconnue
  - Affecte NT4, 2000, XP
- MS02-046
  - Débordement de buffer dans le contrôle ActiveX TSAC
  - Permet l'exécution de code sur le client dans le contexte de l'utilisateur logué

Dernières vulnérabilités
Avis Microsoft (5/5)

EdelWeb

- MS02-047
  - Patch cumulatif pour IE 5.01, IE 5.5 et IE 6
    - Vulnérabilité « gopher:// »
    - Débordement de buffer dans un contrôle ActiveX d'affichage
    - Vulnérabilité XML permettant l'accès à des sources de données distantes
    - Bug d'affichage dans la boîte de dialogue « téléchargement »
    - « Cross-site scripting » via le tag OBJECT
    - « Cross-site scripting » permettant l'ouverture de pages dans la zone « Local Computer »
    - Corrige les contrôles MSN Chat et TSAC
- MS02-048
  - Le contrôle ActiveX « certificats » permet d'effacer des certificats
  - Affecte Windows 98, ME, NT, 2000, XP
- MS02-049
  - Les fichiers FoxPro 6.0 (« .APP ») sont exécutés sans confirmation
- MS02-050
  - Vulnérabilité dans la chaîne de validation des certificats
    - La longueur maximale de la chaîne de confiance n'est pas vérifiée
  - Toute personne possédant un certificat émis par une autorité valide peut devenir autorité intermédiaire de confiance
  - Le risque d'usurpation d'identité est très important
  - Affecte SSL (IE) et S/MIME (Outlook)
  - Microsoft a minimisé cette faille

Dernières vulnérabilités
Autres avis (1/3)

- Vulnérabilité dans Outlook, IE 5.5 et IE 6.0 (MS02-047 ?)
  - Exécution de commandes arbitraires par la redéfinition de l'élément HTML « OBJECT »
  - http://www.pivx.com/larholm/adv/TL003/
- Vulnérabilité dans l'aide Windows 2000
  - « Buffer overflow » dans le contrôle HHCtrl.ocx (utilisé par WinHlp32.exe, IE, Outlook, etc.)
  - Correctif dans le SP3
  - http://online.securityfocus.com/archive/1/285592/2002-08-05/2002-08-11/2
- Mise à jour du composant File Transfer Manager
  - http://transfers.one.microsoft.com/ftm/install

Dernières vulnérabilités
Autres avis (2/3)

- Vulnérabilité MSN
  - Le site groups.msn.com permet l'upload de fichiers
  - Possibilité d'attaques en « cross-site scripting » sur la zone msn.com
  - Affecte toutes les versions de Windows + Office + IE + Outlook
- Vulnérabilité Javascript dans IE 5+ et Netscape 6.2+
  - « Cross-frames scripting »
  - Requière que l'attaquant ait le contrôle d'une machine dans un sous-domaine DNS du site visé
  - http://www.xwt.org/sop.txt
  - Microsoft a annoncé son intention de ne pas corriger cette faille
- Attaque « shatter »
  - Elévation de privilège locale à l'aide de tout service interactif (ex. antivirus)
  - http://security.tombom.co.uk/shatter.html

Dernières vulnérabilités
Autres avis (3/3)

- Disponibilité du SP3 pour Windows 2000 (anglais et français)
- Disponibilité prochaine du SP1 pour Windows XP
- Projet « Palladium » de Microsoft
  - Issu de la guerre de Troie
  - Divers aspects : sandboxes, espaces de stockage chiffrés, etc.
  - Solution software + hardware
  - Publication des sources en conformité avec la loi américaine « DMCA »

Questions / réponses

EdelWeb

- **Questions / réponses**

- **Date de la prochaine réunion :**
  - **Lundi 9 septembre 2002**