EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 8 décembre 2003

Revue des dernières vulnérabilités Microsoft

Nicolas RUFF

nicolas.ruff@edelweb.fr

Dernières vulnérabilités
Avis Microsoft (1/2)

EdelWeb

- **Application de la nouvelle politique de divulgation**
  - Tous les correctifs sortent le 2ème mardi du mois
  - Un correctif par bulletin
  - Un bulletin par type de produit

- **Avis de sécurité Microsoft depuis le 03/11/2003**
  - MS03-048 patch cumulatif pour IE
    - Affecte : IE 5.0 -> 6.0 (Windows ME, NT4 -> 2003)
    - Exploit : 5 nouvelles failles
      - 3 failles "cross-domain"
      - Erreur de zone dans le traitement de fichiers XML
      - "Drag and drop" DHTML
  - MS03-049 débordement de buffer dans le service Workstation
    - Affecte : WKSSVC.DLL (Windows 2000, XP)
    - Exploit : "shell" SYSTEM distant via une fonction vsprintf()
    - Crédit : http://www.eeye.com/

Dernières vulnérabilités
Avis Microsoft (2/2)

- **MS03-050 exécution de macros dans Word / Excel**
  - **Affecte : Office 97 – XP, Works**
  - **Exploit : exécution de macros sans confirmation**

- **MS03-051 débordement de buffer dans les extensions FrontPage**
  - **Affecte : Windows 2000, Windows XP, Office XP**
  - **Exploit :**
    - **Exécution de code sur le serveur via le déboguage à distance**
    - **DoS via SmartHTML**
  - **Crédit : http://www.security-assessment.com/**
  - **Découvert le 30 janvier 2003 !**

- **MS03-050 (re-release)**
  - **Le SP4 de Windows 2000 supprime ce correctif (régression)**
  - **Solution : réappliquer le correctif après le SP**

Dernières vulnérabilités
Infos Microsoft (1/3)

- **4 novembre 2003 : premier hotfix pour Office 2003**
  - **Problème de compatibilité avec les objets créés par une version antérieure de Office Art**
  - **Pas d'impact sur la sécurité**

- **Microsoft expose au musée de la contrefaçon**
  - **http://www.microsoft.com/france/logicieloriginal/info/2003-10-23-nocopy.html**

- **Interview Bill Gates**
  - **http://www.itbusiness.ca/index.asp?theaction=61&sid=53897**
  - **You don't need perfect code to avoid security problems.**
    - **There are things we're doing that are making code closer to perfect, in terms of tools and security audits and things like that. But there are two other techniques: one is called firewalling and the other is called keeping the software up to date. None of these problems (viruses and worms) happened to people who did either one of those things. If you had your firewall set up the right way -- and when I say firewall I include scanning e-mail and scanning file transfer -- you wouldn't have had a problem.**

Dernières vulnérabilités
Infos Microsoft (2/3)

EdelWeb

- **Nombreux changements dans XP SP2**
  - **http://msdn.microsoft.com/library/en-us/dnwxp/html/securityinxpsp2.asp**
    - **ICF en mode "deny all" par défaut**
    - **Clé "RestrictRemoteClients" pour les appels RPC**
    - **Augmentation de la granularité des ACL pour DCOM**
    - **Flag "NoExec" sur les pages de données (requière un AMD K8, AMD64 ou Intel Intanium)**
    - **Traitement des scripts IE dans un espace mémoire isolé**
    - **Traitement des pièces jointes Outlook dans une sandbox**
    - **Tous les correctifs sont compilés avec le flag /GS**
    - **Etc.**

- **Document "la sécurité chez Microsoft"**
  - **http://www.microsoft.com/technet/itsolutions/msit/security/msseccbp.asp**

Dernières vulnérabilités
Infos Microsoft (3/3)

EdelWeb

- **Antivirus et Firewall gratuit pendant 1 an !**
  - Suite "eTrust EZ Armor"
  - En partenariat avec Microsoft
  - http://www.microsoft.com/security/protect/
  - http://www.my-etrust.com/microsoft

- **Gratuit : Microsoft Security Solutions**
  - http://www.microsoftsecuritysolutions.com/Default.asp?id=ros

- **Ouvrage "Windows ou Linux"**
  - Recommandé par Microsoft
  - Écrit par un ex-employé (plus de 10 ans chez Microsoft)
  - http://www.dunod.com/pages/ouvrages/ficheouvrage.asp?Pro_Code_GPE=47982

- **Serveur RMS (Rights Management Service)**
  - http://www.microsoft.com/downloads/details.aspx?FamilyID=be7fae0c-2db2-4f7f-8aa1-416fe1b04fb1&DisplayLang=fr

Dernières vulnérabilités
Autres avis (1/1)

EdelWeb

- **Comportement erratique de OWA 2003**
  - **Affecte : Exchange 2003 + OWA**
  - **Exploit : les utilisateurs peuvent se retrouver redirigés sur des boites aux lettres aléatoires !**
- **5 failles critiques non patchées dans IE**
  - **Affecte : IE 6.0 SP1**
  - **Exploit :**
    - **http://www.safecenter.net/UMBRELLAWEBV4/**
  - **Publiées par "Liu Die Yu"**

Questions / réponses

EdelWeb

- **Questions / réponses**
- **Date de la prochaine réunion :**
  - **Lundi 12 janvier 2003**
- **N'hésitez pas à proposer des sujets et des salles**