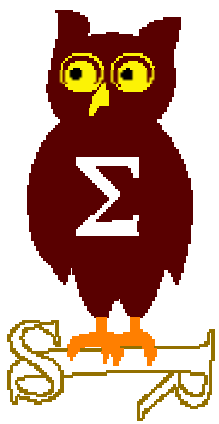
EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 8 novembre 2004



Revue des dernières vulnérabilités Microsoft

Nicolas RUFF

nicolas.ruff@edelweb.fr

Dernières vulnérabilités
Avis Microsoft (1/7)

EdelWeb

- **Avis de sécurité Microsoft depuis le 11 octobre 2004**
  - **Le festival …**
  - **Windows XP SP2 n'est en général pas affecté**
  - **MS04-029 : faille RPC (variante du bogue DCOM)**
    - **Affecte : Windows NT4 uniquement**
    - **Exploit :**
      - **Déni de service, fuite d'information sur le contenu de la mémoire**
      - **Problème dans la fonction rpc__mgmt_inq_stats()**
    - **Crédit : BindView**
  - **MS04-030 : faille dans les messages WebDAV XML**
    - **Affecte : Windows 2000, XP, 2003**
    - **Exploit :**
      - **Déni de service sur IIS**
      - **Publié sur Internet**
    - **Crédit : Sanctum**

Dernières vulnérabilités
Avis Microsoft (2/7)

EdelWeb

- MS04-031 : faille NetDDE ("buffer overflow")
  - Affecte : Windows NT4, 2000, XP, 2003
  - Exploit : exécution de code à distance sous le compte SYSTEM
  - Crédit : NGS

- MS04-032 vulnérabilités Windows multiples
  - Affecte : Windows NT4, 2000, XP, 2003
  - Exploit :
    - Élévation de privilèges vers SYSTEM à travers le gestionnaire de fenêtres ("shatter attack")
    - Élévation de privilèges locale vers SYSTEM à travers la machine virtuelle DOS (VDM)
    - Vulnérabilité dans le traitement des fichiers EMF et WMF (publiée sur Internet en février 2004 !)
    - Déni de service local dans le noyau Windows
  - Crédit :
    - Brett Moore, eEye, Winternals, "hlt"
  - Remarque : possible incompatibilité avec le produit CA Unicenter Software Delivery (USD) version <= 3.1

Dernières vulnérabilités
Avis Microsoft (3/7)

EdelWeb

- **MS04-033 faille Excel**
  - **Affecte : Office 2000, XP, 2001 pour Mac, X pour Mac**
  - **Exploit : "buffer overflow" trivial**
    - **La longueur indiquée d'une chaîne de caractères est utilisée pour copier cette chaîne sans vérification**
  - **Crédit : Brett Moore**

- **MS04-034 faille dans le traitement des fichiers ZIP**
  - **Affecte : Windows XP, 2003**
  - **Exploit : "Buffer overflow", sans doute trivial à exploiter**
  - **Crédit : eEye**

- **MS04-035 faille SMTP**
  - **Affecte : moteur SMTP de Windows XP, 2003, Exchange 2003**
  - **Exploit : "buffer overflow" dans le traitement des réponses DNS**
  - **Crédit : N/D**

Dernières vulnérabilités
Avis Microsoft (4/7)

EdelWeb

- **MS04-036 faille NNTP**
  - **Affecte : Windows NT4 Srv, 2000 Srv, 2003, Exchange 2000, Exchange 2003**
  - **Exploit :**
    - **Publié sur Internet avec moult détails**
    - **"Buffer overflow" dans la commande "XPAT"**
  - **Crédit : Core SDI**

- **MS04-037 faille dans le shell Windows**
  - **Affecte : Windows NT4, 2000, XP, 2003**
  - **Exploit : "buffer overflow" dans des programmes locaux, dont le "convertisseur de groupes de programmes" (un utilitaire de migration Win 3.1 …). Exploitable via une URL.**
  - **Crédit :**
    - **Yorick Koster (ITsec Security Services), Roozbeh Afrasiabi**

Dernières vulnérabilités
Avis Microsoft (5/7)

EdelWeb

- **MS04-038 patch cumulatif pour IE**
  - **Affecte : IE 5.0, 5.5, 6.0 (y compris la version XP SP2)**
  - **Failles corrigées :**
    - **"Heap overflow" dans le traitement des CSS**
    - **"Cross-domain scripting" via des noms de méthode similaires**
    - **"Buffer overflow" dans le moteur d'installation (inseng.dll)**
    - **Faille "drag'n'drop" (publiée en août 2004 et largement exploitée)**
    - **Spoofing d'URL sur les systèmes DBCS**
    - **Spoofing d'URL via le plugin "navigation"**
    - **Téléchargement de fichiers via les "image tags"**
    - **Exécution de scripts via le cache SSL**
  - **Crédit :**
    - **Greg Jones (KPMG), NGS, ACROS Security**

Dernières vulnérabilités
Avis Microsoft (6/7)

EdelWeb

- **Re-release**
  - **MS04-028 Faille GDI+ dite "faille JPEG"**
    - **Raison : mise à jour de la section Office XP, Visio 2002, Project 2002**
    - **Crédit d'origine : Nick DeBaggis**
  - **Mise à jour des outils de détection**
    - **GDI Scan v2 : http://isc.sans.org/gdiscan.php**
    - **Enterprise Scanning Tool Update (cf. Q886988)**
    - **SMS Scanning Tool (cf. Q885920)**
  - **Problème : le code défaillant est partagé par de nombreuses DLLs !**
    - **GDIPLUS.DLL mais aussi MSO.DLL, VGX.DLL, SXS.DLL, ...**

Dernières vulnérabilités
Avis Microsoft (7/7)

EdelWeb

- **Précisions sur la faille "ASP.NET"**
  - **Un scanner a été publié**
    - **http://www.microsoft.com/downloads/details.aspx?FamilyId=BE7366F5-82A1-444F-9EBC-D70B6C8830DD**
  - **Nouvel article mais rien de vraiment neuf**
    - **http://go.microsoft.com/?linkid=1288562**
    - **Installation du module ValidatePath**
    - **Ajout d'un test de normalisation des URLs dans toutes les pages ASP**

Dernières vulnérabilités Infos Microsoft (1/2)

EdelWeb

- Microsoft s'intéresse au problème du Spyware
  - Bill Gates a indiqué que Microsoft travaillait sur une solution
    - http://www.winnetmag.com/Article/ArticleID/44141/44141.html
    - "Mon PC n'a jamais été infecté par un virus, mais j'ai eu des spywares" – Bill G.
  - Sensibilisation en français
    - http://support.microsoft.com/default.aspx?scid=kb;fr-fr;827315
- Chat Cyril Voisin sur 01Net
  - "Dans deux ans, le SP1 ne sera plus supporté et rendra le SP2 indispensable."
    - http://go.microsoft.com/?linkid=1289596
    - http://www.01net.com/article/253323.html
- Le "Virtual Lab" Microsoft
  - http://www.microsoft.com/technet/traincert/virtuallab/isa.mspx

Dernières vulnérabilités
Infos Microsoft (2/2)

EdelWeb

- Exchange 2003 "Best Practices Analyzer"
  - http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=DBAB201F-4BEE-4943-AC22-E2DDBD258DF3
- Le processus de gestion des correctifs en entreprise : méthodes recommandées
  - http://go.microsoft.com/?linkid=1288561
  - Processus de qualification des correctifs
  - Utilisation de MBSA, MSUS ou SMS 2003
- "Microsoft Security Bulletin Advance Notification"
  - Préalerte sur les correctifs de sécurité à J-3
  - http://www.microsoft.com/technet/security/news/bulletinadvance.mspx
  - http://www.microsoft.com/technet/security/bulletin/advance.mspx
  - Ex. en novembre, bulletin "important" sur ISA Server

Dernières vulnérabilités XP SP2 (1/1)

EdelWeb

- Désactiver le Security Center
  - HKLM\SOFTWARE\Microsoft\Security Center
  - Clés de type REG_DWORD :
    - AntiVirusDisableNotify
    - FirewallDisableNotify
    - UpdatesDisableNotify
  - Valeurs
    - 1 = Do Not Display Alert
    - 0 = Display Alert
- Remarque : les détections du Security Center fonctionnent à l'aide de WMI
- La licence DRM de Media Player 10 : intéressant …
  - http://standblog.org/blog/2004/09/03/93113651-drm-wmp-et-cluf-du-sp2-dxp

Dernières vulnérabilités
Autres avis (1/5)

EdelWeb

- Deux failles IE non patchées permettant de contourner les zones de sécurité
  - Affecte : IE 6.0 (y compris XP SP2)
  - Exploit :
    - 1/ Variante "drag & drop"
      - Repose sur la priorité des attributs SRC / DYNSRC dans le tag IMG
    - 2/ Utilisation des fichiers ".hhk" (index d'aide)
  - Crédit : Secunia, http-equiv
  - Code d'exploitation publié sur Internet
    - Utilise la méthode "adodb.recordsets.save"
    - Passablement complexe !
    - http://www.malware.com/noceegar.html
    - http://www.michaelevanchik.com/kara/scrolll/notagain.txt
    - http://www.michaelevanchik.com/kara/scrolll/index.html
  - Workaround : mettre le Kill Bit sur le contrôle "Shell.Explorer"
    - HKLM\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{8856F961-340A-11D0-A96B-00C04FD705A2}]
    - "Compatibility Flags"=dword:00000400

Dernières vulnérabilités
Autres avis (2/5)

EdelWeb

- **Régression dans le traitement des scripts XML par IE**
  - **Réintroduction du bogue MS02-047**
  - **http://www.greymagic.com/security/advisories/gm009-ie/**
- **Bogues dans les navigateurs**
  - **Le focus peut être transféré à tout moment**
    - **http://secunia.com/multiple_browsers_form_field_focus_test/**
  - **Des boites de dialogue peuvent apparaître à tout moment**
    - **http://secunia.com/multiple_browsers_dialog_box_spoofing_test/**
- **Faille dans l'outil CABARC de Microsoft**
  - **Il est possible d'extraire des fichiers hors de la racine en utilisant la syntaxe "../fichier"**
  - **Exploit : http://62.131.86.111/security/cabarc/demo.cab**
  - **Crédit : Jelmer**

Dernières vulnérabilités
Autres avis (3/5)

- Un "fuzzer" pour navigateurs Web
  - http://felinemenace.org/~nd/htmler.py
  - Crashe tous les navigateurs du marché
    - Ex. IE : http://felinemenace.org/~nd/crash_ie/
- Conséquence : un code d'exploitation fiable est disponible dans la nature !
  - Exploit : utiliser un tag IFRAME de plus de 8000 caractères
  - Erreur triviale (utilisation de wcscpy()), corrigée dans le SP2 !
  - http://www.securityfocus.com/bid/11515
- Un Crash Test intéressant pour Windows
  - for %i in (*.exe) do start %i %n%n%n...
  - for %i in (*.exe) do start %i AAAAAA...
- thrashlm : un outil pour effacer les hashes LM
  - http://www.toolcrypt.org/tools/thrashlm/index.html

Dernières vulnérabilités
Autres avis (4/5)

EdelWeb

- De nombreux antivirus traitent incorrectement les fichiers ZIP
  - Affecte :
    - McAfee, Computer Associates, Kaspersky, Sophos, Eset, RAV
    - Des mises à jour sont disponibles
  - N'affecte pas :
    - Symantec, Bitdefender, Trend Micro, Panda
    - Seules les dernières versions ont été testées
  - Exploit :
    - Si taille annoncée du fichier compressé = 0 dans l'entête ZIP, le fichier n'est pas scanné
    - Des virus peuvent ainsi passer sans être détectés
  - Source :
    - iDefense
    - http://www.zdnet.fr/actualites/technologie/0,39020809,39178571,00.htm
- Succès inattendu pour Bagle.AT
  - Rien de révolutionnaire, mais infection massive néanmoins
  - De nombreux CERTs ont émis une alerte

Dernières vulnérabilités
Autres avis (5/5)

EdelWeb

- **Un auteur de spyware arrêté**
  - Sanford Wallace, le "roi du spam"
  - Il fabrique à la fois des spywares et leur antidote (payant) : SpyDeleter
  - http://www.liberation.fr/page.php?Article=244725
- **IE perd des parts de marché**
  - De 95,5% en juin, celle-ci est de 92,9% en octobre
  - N°2 : Firefox (6%)
  - N°3 : Safari et Opera
- **L'image des moniteurs CRT peut être reconstruite à partir de la lumière émise ☺**
  - http://news.com.com/2100-1001-912785.html
  - http://www.cl.cam.ac.uk/~mgk25/
- **"The Source Code Sharing Club"**
  - Disponibilité du code source Cisco Pix 6.3.1
  - Prix : $24,000

Questions / réponses

EdelWeb

- Questions / réponses
- Date de la prochaine réunion
  - Lundi 13 décembre 2004
- N'hésitez pas à proposer des sujets et des salles