EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 9 février 2004

Revue des dernières vulnérabilités Microsoft

Nicolas RUFF

nicolas.ruff@edelweb.fr

Dernières vulnérabilités
Avis Microsoft (1/2)

EdelWeb

- **Avis de sécurité Microsoft depuis le 12/01/2004**
  - **MS04-001 Buffer overflow dans le filtre H323**
    - **Affecte : ISA 2000, SBS 2000, SBS 2003**
    - **Exploit : exécution de code SYSTEM à distance**
    - **Vulnérabilités multi vendeurs reportées par le NISCC**
  - **MS04-002 Élévation de privilèges aléatoire via OWA**
    - **Affecte : OWA / Exchange 2003 en mode backend + frontend**
    - **Exploit : la réutilisation de connexions NTLM sur HTTP fait courir le risque de se retrouver connecté à une boite aux lettres aléatoires**
    - **Vulnérabilité déjà discutée dans les listes et à l'OSSIR mais auparavant non confirmée**
  - **MS04-003 Buffer overflow dans le client MDAC**
    - **Affecte : MDAC 2.5 - 2.8 (Windows 2000 – 2003)**
    - **Exploit : en réponse à un broadcast client, il est possible de faire exécuter du code dans le contexte de sécurité du client**

Dernières vulnérabilités
Avis Microsoft (2/2)

EdelWeb

- MS04-004 Correctif cumulatif pour IE
  - Affecte : IE 5.01, 5.5, 6.0
  - Corrige (au moins) :
    - CAN-2003-01025
      - "Microsoft Internet Explorer does not properly display URLs"
      - Utilisation de %01 dans les URLs
    - CAN-2003-01026
      - "Microsoft Internet Explorer Travel Log Cross Domain Vulnerability"
      - Exécution de scripts dans n'importe quelle zone, y compris Local Machine
    - CAN-2003-01027
      - "Microsoft Internet Explorer Drag-and-Drop Operation Vulnerability"
      - Contrôle du "drag and drop" via une combinaison "SaveRef / window.moveBy"
  - Remarques :
    - Avis de sécurité "out of band"
    - IE ne supporte plus la syntaxe http://user:pwd@host/
      - http://support.microsoft.com/default.aspx?scid=kb;[LN];834489
      - Réactivable par la clé HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE
      - Lister tous les programmes utilisant cette syntaxe

Dernières vulnérabilités
Infos Microsoft (1/1)

EdelWeb

- "Blaster Removal Tool"
  - http://support.microsoft.com/?kbid=833330
- "Office XP/2003 Hidden Data Removal Tool"
  - http://www.microsoft.com/downloads/details.aspx?FamilyID=144e54ed-d43e-42ca-bc7b-5446d34e5360&displaylang=en
- Support Win 98 / 98SE / ME prolongé jusqu'au 30 juin 2006
- MBSA 1.2
  - http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q320454
- Bill Gates
  - "Toute ma fortune ira à des œuvres"
    - Metro 26/01/2004
  - "Les virus et les hackers rendent Windows plus robuste"
    - http://www.theregister.co.uk/content/55/35145.html

Dernières vulnérabilités
Autres avis (1/6)

EdelWeb

- Forte activité virale
  - Ver "Beagle" ou "Bagle"
    - Ver "professionnel", destiné à la collecte d'adresses email
  - Ver MyDoom.A
    - Attaque SCO
  - Ver MyDoom.B
    - Attaque Microsoft
    - Moins virulent car bogué
  - Ver Mimail-R

- Affichage trompeur sous Windows XP
  - #1 Renommer "fichier.exe" en "fichier.folder"
  - #2 Content-Disposition: attachment; filename=malware.{3050f4d8-98B5-11CF-BB82-00AA00BDCE0B}fun_ball_gites_pie_throw%2Empeg
  - Source : http-equiv
  - Pointeurs :
    - http://msdn.microsoft.com/workshop/networking/moniker/overview/appendix_a.asp

Dernières vulnérabilités
Autres avis (2/6)

EdelWeb

- DoS via le partage de fichiers
  - Affecte : Windows XP SP1, Windows 2003 (au minimum)
  - "Memory Leak" intervenant lors de la création/suppression de répertoires avec SmbMount sous Linux
  - Le "pool" système ne peut pas dépasser 343 Mo – au-delà le serveur se bloque
- Cisco affecté par un bug Microsoft
  - Le bug dans le service "Workstation" (MS03-049) provoque un DoS dans les équipements de téléphonie IP
- Suspicion de vulnérabilité (DoS) dans l'implémentation UDP multi-vendeurs
  - http://ntcanuck.com/net/board/index.php?showtopic=175
  - Le CERT a classé l'affaire en "UDP Flood"
  - Le problème pourrait être un déni de service lié à un interblocage dans le traitement des interruptions
  - Aucun autre détail : hoax ?

Dernières vulnérabilités
Autres avis (3/6)

EdelWeb

- Quelques "vieilles" vulnérabilités
  - Internet Explorer
    - Exploit :
      - Le mot clé "expression:" est évalué comme "javascript:"
    - Affecte :
      - Internet Explorer (version non précisée), autres navigateurs non testés
    - Risque de XSS sur les Webmails en cas d'absence de filtrage
  - Message Queuing (MQSVC.EXE)
    - Exploit :
      - "Buffer overflow" exploitable dans le service Message Queuing
    - Affecte :
      - Windows 2000 SP2, SP3 non testé, SP4 corrigé silencieusement !
    - Découvert suite aux déclarations de Jim Allchin (Microsoft)
      - http://www.eweek.com/article2/0,3959,5264,00.asp
  - "Shatter Attack" sur les styles visuels Windows XP
    - Exploit :
      - BCM_GETTEXTMARGIN admet en paramètre un pointeur de type RECT *
      - Il est possible d'injecter du code et de le faire exécuter via ce pointeur
    - Affecte :
      - Toute application privilégiée créant des boutons avec COMCTL32.DLL v6

Dernières vulnérabilités
Autres avis (4/6)

EdelWeb

- "Shatter attack" sur l'aide Windows
  - Exploit :
    - Ouvrir le fichier d'aide d'une application SYSTEM (ex. antivirus)
    - Naviguer vers CMD.EXE à l'aide de la commande "Jump to URL"
  - Affecte :
    - Toute application privilégiée ouvrant un fichier d'aide sans appeler ImpersonateLoggedOnUser()
- Une "fork bomb" pour IE …
  - Exploit :
    - javascript:open('javascript:open(location)')
- Bug dans le Framework .NET
  - Affecte :
    - Framework 1.1 (autres non testés)
  - Exploit :
    - Bogue dans la classe XMLTextReader obligeant à un reboot
  - Chez moi ça ne fonctionne pas (patché silencieusement ?)

Dernières vulnérabilités
Autres avis (5/6)

EdelWeb

- **Droits élevés pour les certificats auto-signés**
  - **Affecte :**
    - **IE / Windows**
  - **Exploit :**
    - **Si un site Web présente un certificat SSL auto-signé et que l'utilisateur clique "oui", ce certificat est ajouté à la liste des CAs avec tous les usages possibles (signature de code, etc.)**

- **Vulnérabilités implémentations IKE**
  - **Affecte :**
    - **Windows + Cisco (code identique)**
  - **Exploit :**
    - **La phase XAUTH (user / password) peut être sniffée et attaquée par dictionnaire**
    - **La phase XAUTH est vulnérable à une attaque MITM**

- **Sanctum possède un brevet sur le pen-test Web**
  - **Brevet n° 6,584,569 posé le 3 mars 2000**
  - **Breveté : le "web crawling", l'analyse de trafic HTTP, la modification de requêtes HTTP, l'analyse des codes d'erreur !**

Dernières vulnérabilités
Autres avis (6/6)

EdelWeb

- Nouvelles pistes de recherche
  - Attaque TOCTOU (Time-Of-Check to Time-Of-Use)
  - Principe :
    - "Race condition" dans la vérification des ACLs
    - Le nom ou le handle de l'objet accédé est changé dynamiquement
  - Aucune application connue pour être vulnérable actuellement
  - http://www.securesize.com/Resources/hookdemo.shtml
  - Remarque : problème connu et corrigé il y a plus de 10 ans sous Unix …

- Finjan Software / Mobile Code Research Center propose 200$ par vulnérabilité non patchée
  - Projet "IE Dream Team"
  - Personnes contactées
    - Georgi Guninski, jelmer, Andreas Sandblad, http-equiv, thePull, Star Dust, Die liu yu.
  - Sujets
    - Java Cellular Security (midlets)
    - Unpatched IE Vulnerabilities
    - Email security (Windows only , Outlook, OWA)
    - Active Content (Windows only: Active X , Java-MS only)
    - HTML, Style, Javascript valuations
    - IE exploits
    - Web mails (exploits code, ways to protect)
    - DOT.NET client security

Questions / réponses

EdelWeb

- Questions / réponses
- Date de la prochaine réunion :
  - Lundi 8 mars 2004
- N'hésitez pas à proposer des sujets et des salles