EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 11 octobre 2004

Revue des dernières vulnérabilités Microsoft

Nicolas RUFF

nicolas.ruff@edelweb.fr

Dernières vulnérabilités
Avis Microsoft (1/1)

EdelWeb

- **Avis de sécurité Microsoft depuis le 13 septembre 2004**
  - **MS04-027 Vulnérabilité dans le convertisseur WordPerfect**
    - **Affecte : Office 2000 / XP / 2003**
    - **Exploit : "buffer overflow" permettant l'exécution de code lors de l'ouverture d'un document WordPerfect dans Office**
      - **Disponible sur Internet**
    - **Crédit : http://www.nextgenss.com/advisories/wordperconv.txt**
  - **MS04-028 Vulnérabilité dans la librairie de décodage JPEG**
    - **Affecte : à peu près tous les logiciels Microsoft …**
    - **Exploit : "heap overflow" dans la librairie GDI+ permettant l'exécution de code à l'ouverture d'un JPEG**
      - **Disponible sur Internet**
    - **Crédit : N/D**
    - **Il existe 26 patches différents, la détection du niveau de patch pose un réel problème à MBSA, SMS, WUS, etc.**
    - **Microsoft fournit un outil spécialisé (gdidettool.exe)**

Dernières vulnérabilités
Infos Microsoft (1/1)

EdelWeb

- **Microsoft diffuse le code source d'Office 2003 aux gouvernements**
  - **http://www.microsoft.com/presspass/press/2004/sep04/09-19OfficeGSPPR.asp**
- **Longhorn prévu pour 2006**
  - **http://www.microsoft.com/france/cp/2004/8/info.asp?mar=/france/cp/2004/8/31080401_a26.html**
  - **Ne sera pas livré avec le système de fichier WinFS**
  - **Améliorations backportées dans XP et 2003**
    - **"Avalon" : interface 3D**
    - **"Indigo" : "grid computing" via HTTP ?**

Dernières vulnérabilités
Autres avis (1/5)

EdelWeb

- **Vulnérabilités multiples dans les implémentations MIME**
  - **Affecte :**
    - **De nombreuses implémentations MIME …**
    - **Avis relayé par le CERT**
  - **Exploit :**
    - **Permet de contourner les filtres en jouant sur des interprétations différentes de la norme entre les logiciels**
  - **Crédit :**
    - **Corsaire**
      - **http://www.corsaire.com/advisories/c030804-00[1-9].txt**
    - **Ce problème avait déjà été analysé l'année dernière par 3APA3A**
      - **http://www.security.nnov.ru/advisories/content.asp**

- **9 failles critiques dans Mozilla !**
  - **Affecte : Mozilla, Netscape, FireFox, ThunderBird**
  - **N'affecte pas : Mozilla 1.7.3+, Firefox 1.0PR+, Thunderbird 0.8+**

Dernières vulnérabilités
Autres avis (2/5)

EdelWeb

- A propos des problèmes de sécurité dans IE XP SP2
  - Lors de l'appel à ShellExecuteEx(), la fonction CSecurityManager::MapUrlToZoneInternal() utilise un cache pour mémoriser le "ZoneID" du composant exécuté
    - Ce cache n'est pas rafraîchi si le composant change de zone
    - La taille du cache est de 4 entrées
  - Le "ZoneID" est stocké dans un Alternate Data Stream
    - Les fichiers extraits d'une archive ZIP par double-click ne sont pas affectés
    - Les fichiers en lecture seule ne sont pas affectés
    - CMD.EXE ignore le ZoneID
- L'installation SP1 + SP2 provoque des permissions dangereuses
  - http://www.pcwelt.de/know-how/extras/103039/
  - Le SP1 autorise le partage de fichiers sur les interfaces Dial-Up, mais ICF est activé par défaut
  - Le SP2 autorise le partage de fichiers sur les interfaces Dial-Up si elle est autorisée sur le LAN
  - SP1 + SP2 => le partage de fichiers est autorisé sur l'interface Dial-Up

Dernières vulnérabilités
Autres avis (3/5)

EdelWeb

- ICF SP2 : le partage de fichiers active automatiquement le PING
  - Utilisé pour mesurer la vitesse de connexion
  - http://support.microsoft.com/default.aspx?scid=kb;en-us;816045
- XP SP2 : les restrictions sur les accès anonymes ne sont pas les mêmes que dans Windows 2003
  - Les droits d'accès "en dur" ont été supprimés
  - Mais il reste possible d'énumérer les comptes anonymement via les exceptions (ex. \pipe\browser)
- Déni de service via un fichier TIFF malformé
  - http://www.securityfocus.com/bid/11202
- Les bogues IE
  - http://www.securityfocus.com/bid/11026
  - http://www.securityfocus.com/bid/11040 (Outlook Express Bcc)
  - http://www.securityfocus.com/bid/11186
  - http://www.securityfocus.com/bid/11200

Dernières vulnérabilités
Autres avis (4/5)

EdelWeb

- **Virus MyFIP : intéressant à plusieurs points de vue**
  - **V1 protégée par MEW**
    - **La routine de décompression contient elle-même un infecteur !**
  - **V2 protégée par ASPACK 2.12**

- **Virus CE.Dust : le code source dévoilé et analysé sur Internet !**
  - **Exploite un bogue Kernel dans Windows Mobile 2003**
  - **http://www.informit.com/articles/article.asp?p=337071**

- **Virus SDBOT.UH : très élaboré techniquement**
  - **Exploite à distance les failles MS03-026, MS02-061, MS03-007, MS04-011**
  - **"Brute force" le compte administrateur local à distance via IPC$**
  - **Déni de service vers des adresses aléatoires**
  - **Installe un sniffer recueillant les chaines "auth", "login", "paypal", …**
  - **Vole les clés de licence pour une quarantaine de jeux en ligne**
  - **Pilotable via IRC**

Dernières vulnérabilités
Autres avis (5/5)

- Le logiciel "FreeGate" détecté comme un Trojan par Symantec
  - http://www.theregister.co.uk/2004/09/14/symantec_targets_freegate/
  - Ce programme est largement utilisé par les Chinois pour contourner les restrictions gouvernementales
- PivX devient PrevX
  - https://www.prevx.com/homeoffice/homeoffice_homedownload.htm
- La société "Securepoint" a engagé Sven Jaschan, auteur du ver Sasser
- AdProtector 1.2
  - Rootkit commercial, destiné aux sociétés de Spyware
  - http://www.randexsoft.com/

Questions / réponses

EdelWeb

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