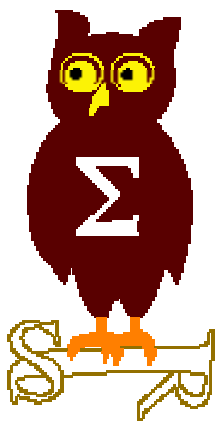
EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 13 septembre 2004



EdelWeb

Revue des dernières vulnérabilités Microsoft

Nicolas RUFF

nicolas.ruff@edelweb.fr

Dernières vulnérabilités
Avis Microsoft (1/5)

EdelWeb

- Avis de sécurité Microsoft depuis le 5 juillet 2004
  - MS04-018 Patch cumulatif pour Outlook Express
    - Affecte : toutes les versions livrées avec Windows NT4 - 2003
    - Exploit : déni de service via entête malformé
      - http://www.securityfocus.com/bid/10711
  - MS04-019 Élévation de privilèges via le gestionnaire d'utilitaires
    - Affecte : Windows 2000
    - Exploit : tout utilisateur pouvant lancer le gestionnaire d'utilitaires (UtilMan.exe) peut acquérir les droits SYSTEM à travers l'aide
      - Code d'exploitation disponible
      - http://www.securityfocus.com/bid/10707
    - Crédit : Cesar Cerrudo (Application Security Inc.)
  - MS04-020 Vulnérabilité dans le système POSIX
    - Affecte : Windows NT4, 2000 (POSIX actif par défaut)
    - Exploit : attaque locale uniquement, permettant d'obtenir les droits SYSTEM
      - Code d'exploitation disponible
      - http://www.securityfocus.com/bid/10710
    - Crédit : Rafal Wojtczuk (McAfee)

Dernières vulnérabilités
Avis Microsoft (2/5)

- **MS04-021 Buffer overflow dans la fonction "redirect"**
  - **Affecte : IIS 4.0**
  - **Exploit : pas d'informations publiées**
    - **http://www.securityfocus.com/bid/10706**
  - **Crédit : Microsoft**

- **MS04-022 Buffer overflow dans le planificateur de tâches**
  - **Affecte : Windows 2000, XP**
    - **Windows NT4 peut être affecté si le planificateur de tâches a été installé avec IE 6**
  - **Exploit : exécution de code dans le contexte de l'utilisateur courant, à la prévisualisation d'un fichier ".job"**
    - **Détails publiés / code d'exploitation disponible**
    - **http://www.securityfocus.com/bid/10708**
  - **Crédit :**
    - **Brett Moore, NGS Software**
    - **http://www.ngssoftware.com/advisories/mstaskjob.txt**

Dernières vulnérabilités
Avis Microsoft (3/5)

EdelWeb

- MS04-023 Vulnérabilité dans l'aide HTML
  - Affecte : Windows 2000, XP , 2003
    - Windows NT4 peut être affecté si IE 6 a été installé
  - Exploit : buffer overflow dans le champ "taille"
    - Détails publiés
    - http://www.securityfocus.com/bid/10705
  - Crédit : Brett Moore

- MS04-024 Vulnérabilité dans la commande "shell:" de Windows
  - Affecte : Windows NT4, 2000, XP, 2003
    - Exploitable dans IE mais aussi Mozilla
  - Exploit :
    - Variante de la faille ADODB, signalée dans la nature
  - Solution de protection alternative :
    - HKLM\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{13709620-C279-11CE-A49E-444553540000}\Compatibility Flags=dword:00000400

Dernières vulnérabilités
Avis Microsoft (4/5)

EdelWeb

- **MS04-025 Vulnérabilités multiples dans IE**
  - **Affecte : IE 5.0, 5.5, 6.0**
  - **Exploit :**
    - **"Integer overflow" dans le traitement des PNG (CAN-2004-0566)**
      - **Vulnérabilité issue de LibPNG ?**
    - **"Double free" dans le traitement des GIF (CAN-2003-1048)**
    - **Pas de changement de contexte de sécurité lors d'un "redirect" (CAN-2004-0549)**
  - **Protège contre le ver "Scob"**
  - **Avis "urgent" (sorti hors planning le 30/07 et mis à jour le 01/08 …)**

Dernières vulnérabilités
Avis Microsoft (5/5)

EdelWeb

- **Août**
  - **MS04-026 "Cross-site scripting" dans OWA sur Exchange 5.5**
    - **Affecte : OWA sur Exchange 5.5**
    - **Exploit : technique "HTTP Response Splitting"**
      - **http://www.securityfocus.com/bid/10902**
      - **http://www.sanctuminc.com/pdf/WhitePaper_HTTPResponse.pdf**
      - **Nécessite d'être authentifié sur OWA**
    - **Crédit : Sanctum Inc.**
  - **MS04-020 Mise à jour de la vulnérabilité POSIX**
    - **Cette vulnérabilité affecte également Interix 2.2**

Dernières vulnérabilités
Infos Microsoft (1/5)

EdelWeb

- **Sortie officielle du SP2 pour Windows XP**
  - **Réactions mitigées**
    - **Nombreuses incompatibilités logicielles**
      - **Principalement dues au Firewall ICF v2 et au flag NX (cf. Q884130)**
  - **Quelques limites**
    - **Nombre de connexions TCP "half-open" sortantes simultanées limitées à 10**
      - **Attention aux mauvaises interprétations**
      - **Le nombre de connexions "totales" est paramétrable par la clé**
        - **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters**
        - **REG_DWORD:TcpNumConnections**
    - **Plus de support des sockets RAW (en émission)**
      - **"We have removed support for TCP sends over RAW sockets in SP2. We surveyed applications and found the only apps using this on XP were people writing attack tools."**
    - **Les applications lancées par CMD ignorent les zones de sécurité**
    - **Temps de login > 20 secondes sur une machine équipée de moins de 256 Mo de RAM**
    - **Un programme peut modifier le statut du Security Center via WMI**
      - **http://www.pcmag.com/article2/0,1759,1639276,00.asp**

Dernières vulnérabilités
Infos Microsoft (2/5)

EdelWeb

- Bloquer/débloquer l'installation du SP2 via Windows Update
  - HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\DoNotAllowXPSP2
  - http://www.microsoft.com/downloads/details.aspx?familyid=8bce6bba-ea5d-4425-89c1-c1cb1ccd463c&displaylang=en
  - http://www.microsoft.com/downloads/details.aspx?familyid=b2300c7b-f3d7-48d6-b86c-1256c0321727&displaylang=en
- Intégrer le SP2 dans un CD d'installation
  - http://www.windows-help.net/windowsxp/winxp-sp2-bootcd.html
  - sp2.exe /integrate:*drive/path*
- Les release notes du SP2
  - http://support.microsoft.com/default.aspx?scid=835935
- Les outils de déploiement
  - http://support.microsoft.com/default.aspx?kbid=838080
- La mise à jour des Support Tools
  - http://support.microsoft.com/default.aspx?kbid=838079
- Les applications bloquées
  - http://support.microsoft.com/default.aspx?kbid=884130

Dernières vulnérabilités
Infos Microsoft (3/5)

EdelWeb

- Retours d'expérience du SANS
  - http://isc.sans.org/xpsp2.php
- Les 20 numéros de série pirate les plus utilisés ont été blacklistés
  - http://www.vnunet.com/news/1155202
- Retours d'expérience du groupe ?

Dernières vulnérabilités
Infos Microsoft (4/5)

EdelWeb

- **Windows XP Security Guide v1.5**
  - Publié le 17 août 2004
  - En anglais uniquement (pour le moment)
- **SP1 pour Office 2003**
  - Corrige également des failles de sécurité
  - http://go.microsoft.com/?linkid=761988
- **WUS : sortie reportée (1er semestre 2005)**
- **Fin de vie pour Windows 2000 Server**
  - http://go.microsoft.com/?linkid=833890
- **Technologie "NAP" (Network Access Protection)**
  - http://www.nwfusion.com/news/2004/0713msnap.html
  - Proche de la solution Cisco "NAC" (Network Admission Control)
  - Technos RADIUS + PEAP + IAS + …
  - Premiers éléments prévus pour Windows 2003 Update

Dernières vulnérabilités
Infos Microsoft (5/5)

EdelWeb

- Quelques liens intéressants
  - Configuration du service de temps (NTP)
    - http://support.microsoft.com/default.aspx?scid=kb;en-us;884776
    - Réponse au spoofing NTP
      - http://www.securityfocus.com/bid/10980
      - http://www.security.nnov.ru/advisories/timesync.asp
  - Introduction à ISA Server 2004 (Webcast)
    - http://go.microsoft.com/?linkid=731825
  - Le processus de gestion des correctifs en entreprise : méthodes recommandées
    - http://go.microsoft.com/?linkid=731827
  - Conception et configuration des services de sauvegarde et de restauration dans les environnements Windows
    - http://go.microsoft.com/?linkid=731828
  - Zoom sur les outils de dépannage de Windows Server 2003
    - http://go.microsoft.com/?linkid=731829
  - Cycle de vie d'un ver : de l'infection à l'éradication
    - http://go.microsoft.com/?linkid=761986

Dernières vulnérabilités
Autres avis (1/6)

- Déni de service dans SMS
  - http://www.securityfocus.com/bid/10726
  - Exploit le port TCP/2702
- Problème de vérification des CRLs
  - Le téléchargement d'une CRL peut complètement bloquer les services X509 en local
  - http://www.securityfocus.com/bid/10901
- Contournement des zones de sécurité dans Outlook 2000/2003
  - Le contenu des balises "OBJECT" non fermées est exécuté sans vérification lorsque l'éditeur de messages par défaut est Word
  - http://www.securityfocus.com/bid/10683
- Communications inter-applets dans la JVM Microsoft
  - Permet de faire bénéficier une Applet des droits d'une autre lancée simultanément
  - http://www.tauwerkkunst.de/javatest/SiteA/CovAppletFNMap.html
  - http://www.securityfocus.com/bid/10688
- Exécution de scripts sans confirmation avec Outlook Express 6.0
  - http://www.securityfocus.com/bid/10692
- Exécution de scripts avec Media Player (Windows 2000)
  - http://www.securityfocus.com/bid/10693

Dernières vulnérabilités
Autres avis (2/6)

EdelWeb

- **Ver Dust.A … pour Windows CE !**
  - Infecte SmartPhones, PocketPC, etc.
  - Se propage par Internet, par email et par échange d'exécutables infectés
  - Pas de charge active
  - Il s'agit d'une "preuve de concept" écrite par le groupe 29A et transmise directement aux éditeurs antivirus
- **Trojan Brador.A pour Windows CE**
  - Ouvre un port et attend les commandes de son créateur
- **Ver Atak**
  - Nouveauté : détecte la présence d'un débogueur actif et s'autodétruit dans ce cas
  - Techniquement peu élaboré
- **Virus RBot-Gr**
  - Donne accès au micro et à la webcam du PC infecté ☺

Dernières vulnérabilités
Autres avis (3/6)

EdelWeb

- **Et toujours … les bugs IE**
  - **Concours du plus petit crash : 11 octets**
    - **"<style>;@/*"**
  - **"What A Drag"**
    - **http://www.malware.com/wattadrag.html**
    - **http://www.malware.com/wottapoop.html (affecte également IE SP2)**
    - **http://www.securityfocus.com/bid/10973**
  - **HijackClick**
    - **http://www.malware.com/paul.html**
    - **http://www.securityfocus.com/bid/10690**
  - **Exploitation de l'association .WSZ (skin Winamp) par du malware (0day)**

Dernières vulnérabilités
Autres avis (4/6)

EdelWeb

- Et autres …
  - http://www.securityfocus.com/archive/1/368671
  - http://www.securityfocus.com/archive/1/368648
  - http://www.securityfocus.com/archive/1/368652
  - http://www.securityfocus.com/archive/1/368650
  - http://www.securityfocus.com/archive/1/368670
  - http://www.securityfocus.com/bid/10627
  - http://www.securityfocus.com/bid/10652
  - http://www.securityfocus.com/bid/10689
  - http://www.securityfocus.com/bid/10694
  - http://www.securityfocus.com/bid/10816
  - http://www.securityfocus.com/bid/10879
  - http://www.securityfocus.com/bid/10943
  - http://www.securityfocus.com/bid/10979

Dernières vulnérabilités
Autres avis (5/6)

EdelWeb

- Les vulnérabilités ne touchent pas que IE
  - Opera <= 7.52 vulnérable à un masquage d'URL
  - Vulnérabilité "shell:" dans Mozilla
  - Etc.
- Remarque : depuis que Mozilla offre 500$ par vulnérabilité, leur nombre a explosé !
- Attaque sur les drivers vidéo ATI et Intel via une image très large (!)
  - http://www.securityfocus.com/bid/10913
- Bogue dans les tunnels IPSEC Windows
  - Le DN n'est pas vérifié
    - Toute personne possédant un certificat de la bonne autorité peut ouvrir un tunnel avec n'importe qui
  - Source : Bugtraq, mai 2004
  - http://www.securityfocus.com/archive/1/347392

Dernières vulnérabilités
Autres avis (6/6)

EdelWeb

- The Source Code Sharing Club
  - http://server.splitto.com.ua/scc/index.html
  - alt.gap.international.sales
- Le "gentil ver" par HP
  - http://www.infoworld.com/article/04/08/18/HNhpscanning_1.html
- Passerez vous le phising test ?
  - http://survey.mailfrontier.com/survey/quiztest.html
- MD5 et SHA-1 en danger, SHA-0 cracké
- Après le spam, le spim …
  - Spam sur messageries instantanées
- OphCrack 1.0, l'outil d'attaque "officiel" des hash LM
  - http://lasecwww.epfl.ch/~oechslin/projects/ophcrack/
- Interview responsable sécurité chez MS
  - http://www.wired.com/wired/archive/12.09/view.html?pg=3
  - "Just this morning I had to install an update to Firefox to block a flaw …"

Questions / réponses

EdelWeb

- **Questions / réponses**
- **Date de la prochaine réunion**
  - **Lundi 11 octobre 2004**
- **N'hésitez pas à proposer des sujets et des salles**