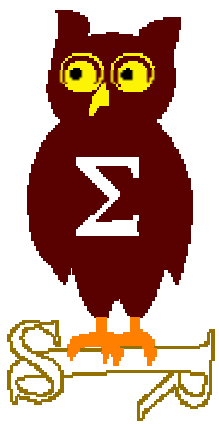
OSSIR
Groupe Sécurité Windows

Réunion du 12 juin 2006



Revue des dernières vulnérabilités Microsoft

Nicolas RUFF

EADS-CCR

nicolas.ruff@eads.net

Dernières vulnérabilités
Avis Microsoft (1/7)

- (Avis de sécurité Microsoft depuis le 10 avril 2006)

- Avril 2006 (5 bulletins, mais 14 failles …)

  - MS06-013 Patch cumulatif pour IE
    - Affecte : IE toutes versions supportées
    - Exploit : corrige 8 failles exploitables à distance, dont CreateTextRange()
    - Crédit : Andreas Sandblad, Jeffrey van der Stad, Jan P. Monsch, Richard M. Smith, Thomas Waldegger, Sowhat, Heiko Schultze, Will Dormann
    - Remarques : plusieurs incompatibilités identifiées, dont Siebel 7

  - MS06-014 Vulnérabilité dans MDAC
    - Affecte : MDAC toutes versions jusqu'à 2.8 SP2
    - Exploit : via l'objet ActiveX "RDS.Dataspace"
    - Crédit : Golan Yosef, Stefano Meller

Dernières vulnérabilités
Avis Microsoft (2/7)

- **MS06-015 Vulnérabilité dans un objet COM**
  - **Affecte : Windows toutes versions supportées**
  - **Exploit : "buffer overflow" dans WebClient**
  - **Crédit : NISCC**

- **MS06-016 "Buffer overflow" à l'ouverture des fichiers .WAB**
  - **Affecte : Outlook Express toutes versions supportées**
  - **Exploit : "buffer overflow"**
  - **Crédit : Stuart Pearson (via ZDI), ATmaCA**

- **MS06-017 "Cross-site scripting" dans les extensions Frontpage**
  - **Affecte : Frontpage 2002 / Sharepoint**
  - **Exploit : "cross-site scripting"**
  - **Crédit : Esteban Martínez Fayó**

Dernières vulnérabilités
Avis Microsoft (3/7)

- **Mai 2006**
  - **MS06-018 Vulnérabilités multiples dans MS-DTC**
    - **Affecte :**
      - **Windows 2000 SP4**
      - **Windows XP SP1 & SP2**
      - **Windows 2003**
    - **Exploit :**
      - **"Buffer overflow" dans CRpcIoManagerServer::BuildContext()**
      - **"Buffer overflow" dans MIDL_user_allocate()**
    - **Crédit : eEye Digital Security, Xiao Chen, Kai Zhang**
    - **Le patch MS05-051 se trompait sur la taille de 8 octets**

Dernières vulnérabilités
Avis Microsoft (4/7)

- MS06-019 "Buffer overflow" dans Exchange Server
  - Affecte :
    - Exchange 2000 SP3+
    - Exchange 2003 SP1 et SP2
  - Exploit : envoyer un email contenant un iCAL ou un vCAL malformé
  - Crédit : Microsoft
  - Patch incompatible avec BlackBerry (!)
- MS06-020 Vulnérabilités multiples dans Flash Player
  - Affecte : Flash Player 6
    - Livré avec Windows 98, 98SE, ME, XP SP1 & SP2
  - Exploit : failles multiples dans le traitement des ".SWF"
  - Corrige : Q910550, Q916208

Dernières vulnérabilités
Avis Microsoft (5/7)

- **Juin 2006**
  - 9 bulletins Windows (allant jusqu'à "Critique")
    - Le correctif de compatibilité Q917425 sera supprimé
  - 1 bulletin Exchange "Important"
    - L'article Q912918 sera mis à jour
  - 2 bulletins Office (allant jusqu'à "Critique")

- **Advisories**
  - Q919637 : 0day dans Word XP/2003

Dernières vulnérabilités
Avis Microsoft (6/7)

- **Révisions**
  - **MS06-005 Vulnérabilité Windows Media Player**
    - **Version 2.0 : nouvelle version du patch**
  - **MS06-014 Vulnérabilité MDAC**
    - **Version 1.1 : précisions**
    - **Version 1.2 : précisions sur la désinstallation**
  - **MS06-015 Vulnérabilité Windows Explorer**
    - **Version 1.1 : incompatibilités identifiées**
      - **HP "Share-to-Web"**
      - **Kerio Personal Firewall**
    - **Version 1.2 : précisions sur la future mise à jour**
    - **Version 2.0 : patch republié le 25/04**
    - **Version 2.1 : pas de patch pour Windows 98/ME**
    - **Nouvel outil d'assistance au déploiement : VERCLSID.EXE**

Dernières vulnérabilités
Avis Microsoft (7/7)

- **MS06-016**
  - **Version 1.2 : incompatibilités identifiées**
- **MS06-019**
  - **Version 1.1 : mise à jour du FAQ**

■ **Remarque**

- **Nombreux problèmes de compatibilité avec MS06-013, 015, 016**
- **http://blogs.technet.com/msrc/archive/2006/04/21/425838.aspx**

Dernières vulnérabilités Infos Microsoft (1/3)

- Les sorties …
  - SQL Server 2005 SP1
  - WSUS SP1
  - "Monad" est devenu Windows PowerShell RC1
  - Versions Beta
    - ISA Server 2006 Beta1
    - Certificate Lifecycle Manager (CLM) Beta1
      - http://www.microsoft.com/windowsserversystem/clm/default.mspx
    - Windows Media 11 Beta
    - Windows Desktop Search 3.0 Beta
    - Office 2007 Beta2
- Vista n'inclura pas de support SecurID natif
  - http://www.zdnet.com.au/news/security/soa/Microsoft_s_token_less_Vista_balances_trust_openness/0,2000061744,39255191,00.htm?feed=rss

Dernières vulnérabilités Infos Microsoft (2/3)

- "Nettoyer les malwares devient impossible"
  - http://www.baselinemag.com/article2/0,1540,1946017,00.asp
- Global Phishing Enforcement Initiative (GPEI)
  - http://www.microsoft.com/presspass/press/2006/mar06/03-20GPEIPR.mspx
  - Plus de 100 actions judiciaires en cours
- Source Fource
  - http://msdn.microsoft.com/events/hero/
- Renforcement du logiciel 'WGA' aux Etats-Unis puis en Europe
- Obligation de publier une version 64-bits des drivers avec Vista
  - Sinon pas d'agrément WHQL

Dernières vulnérabilités
Infos Microsoft (3/3)

- **Le moteur antivirus de Microsoft disponible sur Virus Total**
  - **http://virustotal.com/**
- **Désactiver complètement UAC dans Vista**
  - **http://blogs.msdn.com/uac/archive/2006/01/22/516066.aspx**
- **Microsoft Standard User Analyzer**
  - **http://www.microsoft.com/downloads/details.aspx?familyid=df59b474-c0b7-4422-8c70-b0d9d3d2f575&displaylang=en**

Dernières vulnérabilités
Autres avis (1/10) – failles

- **Attaques ciblées utilisant un 0day Word (W32/Ginwui.A)**
  - Rebond via des sites Chinois : 3322.org, scfzf.xicp.net
  - Affecte au moins : Word XP, Word 2003
  - Le problème se situerait dans les "Smart Tags"
  - A rapprocher de ce post ?
    - http://archives.neohapsis.com/archives/vuln-dev/2006-q2/0038.html
  - Workaround : "winword.exe /safe"
- **Attaque GREENAPPLE chez Immunity**
  - Exploitation distante d'un bogue noyau dans SMB.SYS
  - Exploit pour une ancienne faille (MS05-011)

Dernières vulnérabilités
Autres avis (2/10) – failles

- **Faille critique dans RealVNC 4.1.1**
  - **Il n'est pas nécessaire de connaître le mot de passe pour se connecter !**
  - **http://www.intelliadmin.com/blog/2006/05/vnc-flaw-proof-of-concept.html**
- **0day Java (testé)**
  - **http://www.illegalaccess.org/exploit/ObjectStackOverflow.html**
- **Microsoft change subrepticement le support du fichier "hosts"**
  - **Domaines non redirigeables :**
    - **www.msdn.com msdn.com www.msn.com msn.com go.microsoft.com msdn.microsoft.com office.microsoft.com microsoftupdate.microsoft.com wustats.microsoft.com support.microsoft.com www.microsoft.com microsoft.com update.microsoft.com download.microsoft.com microsoftupdate.com windowsupdate.com windowsupdate.microsoft.com**

Dernières vulnérabilités
Autres avis (3/10) – failles

- **Inclusion de fichiers via le tag "mailto:"**
  - **Affecte : Office 2003 (toutes versions)**
  - **Exploit : "mailto:../../../<fichier sensible>**

- **"Heap overflow" dans MS Infotech Storage System**
  - **Affecte : Windows 2000 SP4, XP SP1 & SP2**
  - **Exploit : ouverture d'un fichier .CHM par "itss.dll"**
  - **Crédit : Rubén Santamarta**

- **"Heap overflow" dans les fichiers ".HLP"**
  - **http://www.open-security.org/advisories/15**

- **Nombreuses implémentations DNS vulnérables**
  - **Outil de fuzzing de l'université OULU (bien connue dans le domaine)**

Dernières vulnérabilités
Autres avis (4/10) – failles IE

- **Patch MS05-054 incomplet**
  - Affecte : IE 6 (autres versions non testées)
    - Versions Windows XP SP1 et Windows 2003 SP0 en particulier
    - Version Windows XP SP2 moins vulnérable grâce à la barre d'information
  - Exploit :
    - "Condition temporelle" permettant de contourner les boites de confirmation
    - Exploitation difficile

- **Bogue IE dans le support des tags "OBJECT"**
  - Affecte : IE 6 (autres versions non testées)
  - Exploit :
    - perl -e '{print "<STYLE></STYLE>\n<OBJECT>\nBork\n"x32}' >test.html
    - Exploitation difficile

- **"Cross-domain scripting"**
  - Affecte : IE 6 (autres versions non testées)
  - Exploit :
    - Exploitation des URLs mhtml://
    - Cf. http://www.frsirt.com/bulletins/4914

Dernières vulnérabilités
Autres avis (5/10) – failles IE

- **Un bug étrange …**
  - Créer un raccourci sur le bureau
    - Vers n'importe quelle application (ex. CALC.EXE)
  - Renommer le raccourci en adresse Internet valide
    - Ex. www.microsoft.com
  - Taper l'adresse dans Internet Explorer

- **Evénement "keystroke" permettant d'uploader des fichiers**
  - Affecte : IE toutes version
  - http://www.frsirt.com/bulletins/5518

Dernières vulnérabilités
Autres avis (6/10) – virus et spywares

- **OpenOffice plus dangereux que MS Office ?**
  - **http://www.f-secure.com/weblog/archives/openoffice_security.pdf**
  - **Cf. également présentation de E. Filiol au SSTIC'06**
  - **PoC : StarDust.A**
- **Exemple de Toolkit permettant de réaliser des sites hostiles**
  - **http://www.websense.com/securitylabs/alerts/alert.php?AlertID=472**
  - **Disponible pour $20**

Dernières vulnérabilités
Autres avis (7/10) – virus et spywares

- La Chine adopte une législation anti-spam
  - Il est interdit de posséder un serveur SMTP sans autorisation
  - Toute personne envoyant du mail doit être authentifiée
  - Les emails doivent être archivés pendant 60 jours
  - http://www.vnunet.com/vnunet/news/2154063/china-outlaws-outlook
- Un bogue trouvé dans GCC grâce au virus "Bi.a"
  - http://software.newsforge.com/article.pl?sid=06/04/18/1941251
  - http://www.pcworld.com/news/article/0,aid,125461,00.asp
- Un virus Matlab ☺
  - Nom de code "Bagoly"
  - Fichier ".m"

Dernières vulnérabilités
Autres avis (8/10) – virus et spywares

- **Nettoyer Look2Me : mission impossible ?**
  - Enlève le privilège SeDebug à l'administrateur
  - S'installe comme "Notification Package" dans WINLOGON
- **"Nugache" : un nouveau type de bot**
  - Se propage par AIM
  - Utilise le P2P comme canal de C&C
- **Problème de conversion entre noms longs et 8.3**
  - http://www.securityfocus.com/bid/17934/info
  - Permet d'éviter le scan antivirus
  - Exemple de produits vulnérables
    - Norton AV, Kaspersky AV, AVG AV, Norman AV, Ad-Aware, Spybot Search&Destroy

Dernières vulnérabilités
Autres avis (9/10)

- **L'Australie signe un accord avec Microsoft**
  - **http://australianit.news.com.au/articles/0,7204,18699718%5E15306%5E%5Enbv%5E,00.html**
  - **Inclus accès au code source Windows et création d'une équipe d'urgence**
  - **Autre pays déjà signataires : USA, Canada, Chili et Norvège**
- **Reprise des travaux sur la DADVSI**
  - **Nombreux amendements en cours**
  - **Durcissement général**
    - **Plus de plateforme pour les artistes indépendants**
    - **Distinction entre P2P et autres protocoles**
    - **Plus de notion d'interopérabilité**
    - **Création d'un registre public des œuvres protégées**
    - **Recours au tribunal supprimé pour les citoyens mais conservé pour les majors (?)**
    - **Obligation pour tout propriétaire d'une connexion internet à mettre en place des moyens de sécurisation proposés par son FAI (???)**
  - **Le gouvernement a cédé devant Apple (entre autres)**
    - **http://news.zdnet.com/2100-9588_22-6071478.html**

Dernières vulnérabilités
Autres avis (10/10)

- **Nouvelles attaques sur les DNS**
  - Empoisonnement du ".com" par serverhome.com (65.23.154.2)
- **Un internet à 2 vitesses ?**
  - http://www.liberation.fr/page.php?Article=386943
  - Les services payants (ex. VOD) auraient droit à un QoS supérieure contre abonnement
- **SpamOrHam : classifier 92,000 messages à la main …**
  - http://www.extravalent.com/spamorham/

Questions / réponses

- Questions / réponses
- Date de la prochaine réunion
  - Prochaine réunion 10 juillet 2006
- N'hésitez pas à proposer des sujets et des salles