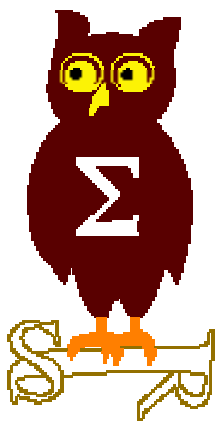
OSSIR
Groupe Sécurité Windows

Réunion du 12 septembre 2005



Revue des dernières vulnérabilités Microsoft

Nicolas RUFF

EADS-CCR

nicolas.ruff@eads.net

Dernières vulnérabilités
Avis Microsoft (1/8)

- (Avis de sécurité Microsoft depuis le 11 juillet 2005)

- Juillet 2005
- Bulletins "critiques"
  - MS05-035 "buffer overflow" dans Word
    - Affecte : Word 2000, Word 2002, Works 2000-2004
    - Exploit : "Unicode buffer overflow" à l'ouverture d'un ".DOC"
    - Crédit : Lord Yup + iDefense
  - MS05-036 "buffer overflow" dans la gestion des profils de couleur
    - Affecte : Windows 2000, XP, 2003 (tous Service Packs)
    - Exploit : "buffer overflow" dans le traitement des profils de couleur, exploitable via un site Web ou un email
    - Crédit : Shih-hao Weng

Dernières vulnérabilités
Avis Microsoft (2/8)

- MS05-037 Vulnérabilité "JView Profiler"
  - Affecte : JVM intégrée dans
    - Windows 2000 SP4
    - Windows XP SP0/SP1/SP2
    - Windows 2003 SP0/SP1
  - Exploit : exécution de code via une applet Java
  - Crédit : -

- Août 2005
- Bulletins "critiques"
  - MS05-038 Patch cumulatif pour IE
    - Affecte : IE (toutes versions)
    - Exploit :
      - "Buffer overflow" via une image JPEG
      - "Cross-site scripting" (XSS) via WebDAV
      - "Buffer overflow" dans le composant scriptable DEVENUM.DLL
    - Crédit :
      - Bernhard Mueller / Martin Eiszner (SEC Consult)
      - NSFOCUS

Dernières vulnérabilités
Avis Microsoft (3/8)

- MS05-039 Vulnérabilité "Plug and Play"
  - Affecte :
    - Windows 2000 SP4
    - Windows XP SP1/SP2
    - Windows 2003 SP0/SP1
  - Exploit : exécution de code à distance sous le compte SYSTEM
    - Exploitable de manière anonyme via RPC sous Windows 2000
    - Exploitable par un utilisateur authentifié via RPC sous Windows XP SP1
    - Exploitable par un administrateur local sous Windows XP SP2 / Windows 2003
  - Crédit :
    - Neel Mehta (ISS X-Force)
    - Jean-Baptiste Marchand (HSC)
  - Exploité par le(s) ver(s) "Zotob"

- MS05-043 Vulnérabilité dans le spooler d'impression
  - Affecte :
    - Windows 2000 SP4
    - Windows XP SP1/SP2
    - Windows 2003 SP0
  - Exploit : exécution de code à distance sous le compte SYSTEM
  - Crédit : Kostya Kortchinsky (CERT Renater)

Dernières vulnérabilités
Avis Microsoft (4/8)

- **Bulletins "importants"**
  - **MS05-040 Vulnérabilité dans le service TAPI**
    - **Affecte :**
      - **Windows 2000 SP4**
      - **Windows XP SP1/SP2**
      - **Windows 2003 SP0/SP1**
    - **Exploit : exécution de code à distance sous le compte SYSTEM**
      - **Exploitable de manière anonyme via RPC sous Windows 2000 Server**
      - **Exploitable localement sous Windows 2000 Pro / XP**
      - **Exploitable par un utilisateur authentifié via RPC sous Windows 2003**
    - **Crédit : Kostya Kortchinsky (CERT Renater)**
  - **MS05-041 DoS via RDP**
    - **Affecte :**
      - **Windows XP SP1/SP2**
      - **Windows 2003 SP0/SP1**
    - **Exploit : un paquet malformé provoque un écran bleu**
    - **Crédit : Tom Ferris (Security Protocols)**
    - **Anciennement connu sous :**
      - **http://go.microsoft.com/fwlink/?LinkId=50422**

Dernières vulnérabilités
Avis Microsoft (5/8)

- MS05-042 Vulnérabilités Kerberos multiples
  - Affecte :
    - Windows 2000 SP4
    - Windows XP SP1/SP2
    - Windows 2003 SP0/SP1
  - Exploit :
    - Fuite d'information, déni de service, spoofing d'identité via PKINIT
    - Exécution de code à distance sous le compte SYSTEM ?
      - Sur un contrôleur de domaine (port TCP/88 et UDP/88)
  - Crédit :
    - Tony Chin (Shell, Inc.)
    - Andre Scedrov + students (Pennsylvania University)

Dernières vulnérabilités
Avis Microsoft (6/8)

- **Septembre 2005**
  - **Pas de bulletins de sécurité**
  - **Bulletins "non sécurité"**
    - **Microsoft Update (MU)**
    - **Windows Update (WU)**
    - **Windows Server Update Services (WSUS)**
    - **Software Update Services (SUS)**

Dernières vulnérabilités
Avis Microsoft (7/8)

- Révisions
  - MS05-019
    - 2.1 : mise à jour des effets de bord
  - MS05-023
    - 2.0 : Word Viewer est affecté également
  - MS05-030
    - 1.2 : ce bulletin ne remplace pas MS04-018
  - MS05-032
    - 2.0 : nouveau correctif pour XP64 et Windows 2003
  - MS05-033 Vulnérabilité dans le client Telnet
    - 2.0 : publication d'un correctif pour SFU 2.0 et 2.1
  - MS05-036 "Buffer overflow" dans les profils ICC
    - 1.1 : cas où le redémarrage requis
  - MS05-037 Vulnérabilité "JView Profiler"
    - 1.1 : mise à jour des méthodes de détection
  - MS05-038 Patch cumulatif pour IE
    - 2.1 : mises à jour variées
  - MS05-040 Vulnérabilité dans le service TAPI
    - 1.1 : mise à jour de la section Windows 98/ME
  - MS05-043 Vulnérabilité dans le spooler d'impression
    - 1.1 : mise à jour des "workarounds"

Dernières vulnérabilités
Avis Microsoft (8/8)

- **Alertes**
  - **[Q899588] Ver Zotob**
    - **Exploite la faille PnP**
  - **[Q906267] "0day" publié sur MSDDS.DLL**
    - **Affecte : composant ActiveX MSDDS installé par Visual Studio et/ou Office**
    - **Exploit : "heap overflow" ?**
  - **[Q906574] "Clarification of Simple File Sharing and ForceGuest"**
    - **Précise les conditions d'exploitabilité de MS05-039**
  - **[Q897663] Il est possible de créer des exceptions dans le firewall XP SP2 sans confirmation de l'utilisateur**
  - **[Q840123] Déni de service sur Exchange 2003 via un accès IMAP4**

Dernières vulnérabilités
Infos Microsoft (1/4)

- **Windows XP "N"**
  - Version "allégée" de Windows XP (suite aux procès anti-trust)

- **Les sorties en Beta 1**
  - Windows Longhorn alias "Vista"
  - WinFS (système de fichiers structuré)
  - "Acrylic" (programme de dessin de la suite Office)
  - Microsoft Shell alias "Monad"
  - Le shell MSH intéresse déjà les auteurs de virus
    - http://www.zdnet.fr/actualites/informatique/0,39040745,39250635,00.htm

- **Publication de MBSA 2.0**
  - http://www.microsoft.com/technet/security/tools/mbsahome.mspx
  - Supporte entre autres :
    - Windows 2000+ SP3
    - Office XP+
    - Exchange 2000+
    - SQL Server 2000 SP4+

- **Une version 2 du SRP1 pour Windows 2000 en cours d'élaboration**
  - http://support.microsoft.com/kb/891861
  - Sortie en beta le 13 septembre

Dernières vulnérabilités
Infos Microsoft (2/4)

- Comment utiliser la sécurité comme publicité
  - http://go.microsoft.com/?linkid=3783138
  - "Read how Microsoft SQL Server 2000 on Windows Server 2003 experienced 144 fewer security vulnerabilities versus Oracle 10g on Red Hat Enterprise Linux 3.0"
- "Cell phone virus threats: why they shouldn't be dismissed"
  - http://www.microsoft.com/smallbusiness/resources/technology/security/cell_phone_virus_threats_why_they_shouldnt_be_dismissed.mspx
- Microsoft envisage de racheter la société Claria
  - Auteur du célébrissime spyware "Gator" (livré avec le codec DivX)
  - En tout cas le "threat level" de Gator a diminué dans MS AntiSpyware ☺
- Le plus jeune MCP Microsoft a … 9 ans
  - http://blogs.msdn.com/somasegar/archive/2005/07/13/438647.aspx
- Le projet "Microsoft HoneyMonkey" identifie 752 pages Web qui installe du code via un "0day" dans IE
  - http://www.securityfocus.com/news/11273

Dernières vulnérabilités
Infos Microsoft (3/4)

- Microsoft invente "Avalanche" pour contrer Bittorrent
  - http://www.research.microsoft.com/~pablo/avalanche.aspx
- "Windows Genuine Advantage" (WGA)
  - Désormais obligatoire pour aller sur WindowsUpdate
    - Les mises à jour automatiques continuent à fonctionner
  - Possède un check spécifique "anti WINE"
    - Mais la clé de base de registre utilisée pour le test a été supprimée ☺
  - Cracké en 24h …
    - Au moins 3 méthodes connues
      - "Patcher" la DLL de vérification
      - javascript:void(window.g_sDisableWGACheck='all')
      - Désactiver les ActiveX

Dernières vulnérabilités
Infos Microsoft (4/4)

- **Microsoft déclare la guerre à Google**
  - **Programme "Web 2.0"**
    - **Accès à MSN Search via SOAP**
    - **Ouverture des API**
      - **Microsoft Desktop Search**
      - **MSN Virtual Earth**
      - **MSN Messenger**

Dernières vulnérabilités
Autres avis (1/7)

- **Usurpation du SERVER_NAME**
  - Affecte : IIS 5.0, 5.1, 6.0
  - Exploit : la variable SERVER_NAME est positionnée en fonction du header HTTP renvoyé par le client
  - Crédit : http://ingehenriksen.blogspot.com/

- **"Directory Traversal" permettant de lancer des exécutables sous le process INETINFO.EXE**
  - Affecte : IIS 5.x
  - Exploit : http://localhost/%20c:/windows/system32/notepad.exe
  - Crédit : http://ingehenriksen.blogspot.com/

- **DoS sur ASP.NET**
  - Affecte : pages ASP.NET
  - Exploit : la fonction System.Xml.Serialization ne filtre pas correctement ses paramètres et peut utiliser 100% du CPU
  - Crédit : Bryan Sullivan, Sacha Faust (SPI Dynamics)

- **"Buffer overflow" dans la préauthentification du client DameWare**
  - La société est basée à "Mandeville, LA" près de la Nouvelle-Orléans donc pas de patch à attendre dans les prochaines semaines …

Dernières vulnérabilités
Autres avis (2/7)

- Un autre problème méconnu de ASP.NET : une mauvaise utilisation de VIEWSTATE
  - http://scottonwriting.net/sowblog/posts/3747.aspx
  - Exemple de victime : MS GateKeeper Security Test
    - http://www.theregister.co.uk/2005/05/11/ms_gatekeeper_test_fiasco
- Faille dans REGEDIT
  - Les clés de base de registre dont les données font entre 256 et 260 octets sont invisibles !
  - La voie royale pour les virus
- Astuce FireFox
  - http://http:// renvoie sur la première réponse Google pour "http"
  - C'est-à-dire :
    - "http" -> Microsoft
    - "https" -> PayPal
  - http://http://toto exploitable pour du phishing ?

Dernières vulnérabilités
Autres avis (3/7)

- "TCP Zombie Attack"
  - Affecte : de nombreuses implémentations TCP/IP dont Windows
  - Exploit : en envoyant un paquet ACK avec un numéro de séquence invalide, il est possible de faire générer à la victime énormément de trafic
  - http://www.securityfocus.com/bid/13215
- Rejet de la directive sur les brevets logiciels au parlement européen
  - A une très large majorité
- The "0day" initiative
  - http://www.zerodayinitiative.com/
  - Une bourse au "0day", organisée par 3Com / TippingPoint
- iDefense (le plus gros acheteur public de "0day") a été racheté par Verisign
  - Conséquences :
    - Le prix du "0day" a doublé
    - A travers le programme "Growth", il est possible d'avoir un salaire annuel

Dernières vulnérabilités
Autres avis (4/7)

- DoS sur ActiveSync
  - Affecte : ActiveSync <= 3.7.1
  - Exploit : connexions multiples sur le port TCP/5679
- Cisco + ISS vs. Michael Lynn
  - "Exploitation fiable des Heap Overflow sous IOS"
    - Présenté à BH US 2005
    - Violation d'un NDA concernant le code source Cisco ?
    - http://www.securityfocus.com/news/11259
  - McAfee prétend avoir une signature dans son IDS
    - http://www.mcafeesecurity.com/us/about/press/corporate/2005/20050803_181545.htm
- Compromission de la base d'utilisateurs du site Cisco.com
  - http://software.silicon.com/security/0,39024655,39150991,00.htm
  - Peu de temps après la conf' ☺

Dernières vulnérabilités
Autres avis (5/7)

- Virus "PGPCoder"
  - Chiffre tous les fichiers .DOC / .XLS / etc. par PGP
  - L'auteur demande une rançon pour envoyer la clé privée
- Références croisées (multi vendeurs) des virus "dans la nature"
  - Dispo sur http://www.av-test.org/
- Retour d'un vieux bug dans Symantec AntiVirus
  - Affecte : Symantec AntiVirus 9 < MR3
  - Exploit : "shatter attack" dans le bouton droit / "scan for viruses"
  - Remarques :
    - Bug corrigé dans les versions 7.5.1b62 et 7.6.1b35a
    - Exemple parfait de "shatter attack" (il suffit de faire F1 pour exploiter)
- Une faille IE exploitable à venir …
  - http://www.security-protocols.com/modules.php?name=News&file=article&sid=2891

Dernières vulnérabilités
Autres avis (6/7)

- **Inutile … donc indispensable !**
  - **http://www.hexview.com/vmaps.html**

Dernières vulnérabilités
Autres avis (7/7)

- Le classement du SANS (vulnérabilités les plus dangereuses du 2ème trimestre)
  - http://www.sans.org/top20/q2-2005update/detail.php
  - Produits Microsoft
    - Microsoft Internet Explorer Multiple Vulnerabilities (MS05-020)
    - Microsoft Internet Explorer Multiple Vulnerabilities (MS05-025)
    - Microsoft Exchange Server Extended Verb Overflow (MS05-021)
    - Microsoft Windows Message Queuing Service Overflow (MS05-017)
    - Microsoft Windows SMB Protocol Processing Overflow (MS05-027)
    - Microsoft Windows HTML Help File Parsing Overflow (MS05-026)
    - Microsoft Windows Shell Remote Code Execution (MS05-016)
  - Autres
    - Computer Associates BrightStor ARCServe Backup Overflow
    - Veritas Backup Software Multiple Vulnerabilities
    - Computer Associates and Zone Alarm Vet Library Overflow
    - Oracle Cumulative Update April 2005
    - RealNetworks RealPlayer Multiple Vulnerabilities
    - Apple iTunes MPEG4 File Processing Overflow
    - Mozilla and Firefox Browsers Multiple Vulnerabilities
    - Apple Cumulative Security Update 2005-005
    - Apple Cumulative Security Update 2005-006

Questions / réponses

- **Questions / réponses**
- **Date de la prochaine réunion**
  - **Lundi 10 octobre 2005**
- **N'hésitez pas à proposer des sujets et des salles**