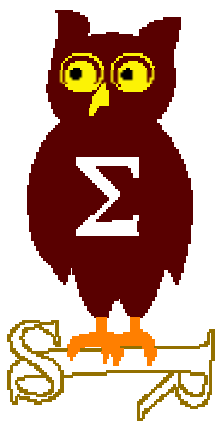
OSSIR
Groupe Sécurité Windows

Réunion du 10 avril 2006



Revue des dernières vulnérabilités Microsoft

Nicolas RUFF

EADS-CCR

nicolas.ruff@eads.net

Dernières vulnérabilités
Avis Microsoft (1/3)

- (Avis de sécurité Microsoft depuis le 13 mars 2006)

- Mars 2006
  - MS06-011 Durcissement des ACLs sur les services
    - Affecte : Windows XP SP1, Windows 2003 SP0
    - Exploit : attaque "WinVal"
  - MS06-012 Correctifs multiples pour Office
    - Affecte : Office 2000/XP/2003, Works, Office pour Mac
    - Exploit : plusieurs failles critiques permettant d'exécuter du code à l'ouverture d'un document
    - Crédits : multiples

- Avril 2006
  - 4 bulletins Windows allant jusqu'à "critique"
    - Correctif pour "CreateTextRange"
  - 1 bulletin Office + Windows "modéré"

Dernières vulnérabilités
Avis Microsoft (2/3)

- **Advisories**
  - **Q912945**
    - **Mise à jour "non sécurité" pour IE -> sera intégrée au correctif Q917077**
  - **Q916208**
    - **Mise à jour disponible pour la vulnérabilité Flash**
  - **Q914457**
    - **ACLs permissives sur les services corrigées par MS06-011**
  - **Q917077**
    - **"Buffer overflow" via createTextRange() dans IE**
    - **Largement exploité dans la nature (0-day)**
    - **Patch "non officiel"**
      - **http://www.determina.com/security_center/security_advisories/securityadvisory_march272006_1.asp**
    - **Mise à jour ultérieure de ce composant prévue pour Juin**

Dernières vulnérabilités
Avis Microsoft (3/3)

- **Révisions**
  - **MS06-012**
    - **Version 1.2 : clarifications**
  - **MS06-007**
    - **Version 1.1 : précision sur la clé de base de registre créée**
  - **MS06-007**
    - **Version 1.2 : patch non cumulatif avec MS05-019 sur Windows 2003 SP1**
  - **MS05-013**
    - **Version 1.3 : évolution du modèle ActiveX**

Dernières vulnérabilités
Infos Microsoft (1/2)

- **Microsoft et l'université du Michigan s'associent pour présenter un rootkit totalement furtif**
  - **Lance une machine virtuelle avant le système d'exploitation**
  - **http://www.eweek.com/article2/0,1895,1936666,00.asp**
- **Fin de la Beta pour Monad**
- **Windows Desktop Search 2.6.5 (beta)**
  - **http://www.microsoft.com/downloads/details.aspx?familyid=971793F2-95AC-4788-8006-92D848E67A40&displaylang=en**
- **Site officiel du projet Strider HoneyMonkey**
  - **http://research.microsoft.com/HoneyMonkey/**
- **Anti-XSS Library 1.0**
  - **http://www.microsoft.com/downloads/details.aspx?familyid=9A2B9C92-7AD9-496C-9A89-AF08DE2E5982&displaylang=en**

Dernières vulnérabilités
Infos Microsoft (2/2)

- "The software giant announced last week that Mike Nash, head of Microsoft's Security Technology Unit (STU), will step down from his position to go on sabbatical."
  - http://www.scmagazine.com/uk/news/article/550420/nash-go-sabbatical-Redmond/

- Virtual Server 2005 R2 disponible gratuitement
  - http://www.microsoft.com/windowsserversystem/virtualserver/default.mspx
  - Remarques :
    - Supporte officiellement Linux (Red Hat et Suse) – via Microsoft Connect
    - VMWare Server Beta 2 est également gratuit

Dernières vulnérabilités
Autres avis (1/4) - failles

- FrSIRT (ex. K-Otik) ne distribue plus les exploits gratuitement
  - http://www.eweek.com/article2/0,1895,1938511,00.asp
- "Buffer overflow" dans ILASM et ILDASM
  - Affecte : .NET Framework < 2.0 (pas de patch)
  - Exploit : nécessite que la victime utilise les outils ILASM ou ILDASM ! (peu réaliste)
- Analyse des temps d'exploitation par le HoneyNet norvégien
  - http://www.honeynor.no/research/time2exploit/
  - Moyenne = 77 jours
  - Médiane = 5 jours
- Une nouvelle faille IE permettant le spoofing d'adresse
  - "Race condition" dans le chargement de Flash
  - http://secunia.com/advisories/19521/

Dernières vulnérabilités
Autres avis (2/4) – virus et spywares

- **Bagle.GI**
  - Chaque version envoyée par endoliteindia.com est différente
  - Utilisation de ASProtect
- **MSIL.Letum.A**
  - Virus pour Windows *et* Windows Mobile écrit en .NET
  - http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FLETUM%2EA&VSect=T
- **Un autre virus multi-plateformes (Windows / Linux)**
  - http://www.viruslist.com/en/weblog
- **Microsoft inclut Alcan.B dans le Malicious Removal Tool de février**
  - 7 mois après la détection de ce virus, 250 000 machines sont encore contaminées
  - http://blogs.technet.com/antimalware/

Dernières vulnérabilités
Autres avis (3/4) – virus et spywares

- L'adware "Coolwebsearch" change d'adresse IP (85.249.23.x)
- Hacker Defender arrête le service "anti détection"
- Un virus RFID ?
  - http://www.rfidvirus.org/
  - Il est possible de réaliser des injections SQL via le nom d'un tag (limité à 128 caractères)
- Un nouveau groupe anti-phishing : PIRT
  - http://wiki.castlecops.com/PIRT
- "Web Hacking Incident Database"
  - http://www.webappsec.org/projects/whid/

Dernières vulnérabilités
Autres avis (4/4)

- **Adoption de la DADVSI**
  - **Plusieurs questions en suspens …**
    - **Mise à disposition de logiciel de P2P interdite**
    - **Contournement des "mesures techniques de protection" interdit**
    - **"Backdoor" dans les réseaux universitaires**
    - **Remise en cause de la copie privée**
    - **Exigence d'interopérabilité => iTunes pourrait se retirer du marché français …**

- **Décret sur la conservation des données (26 mars)**
  - **Durée : 1 an**

- **Yahoo!**
  - **"Yahoo: We need effective cybercrime laws"**
  - **http://news.com.com/Yahoo+We+need+effective+cybercrime+laws/2100-7348_3-6056523.html?tag=nefd.top**

- **Jigsaw vous propose d'acheter ou vendre des numéros de téléphone**
  - **http://www.jigsaw.com/**

Questions / réponses

- Questions / réponses
- Date de la prochaine réunion
  - JSSI le 22 mai 2006 (venez nombreux)
  - Prochaine réunion 12 juin 2006
- N'hésitez pas à proposer des sujets et des salles