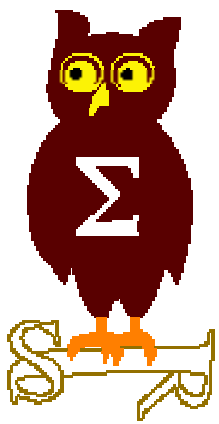
OSSIR
Groupe Sécurité Windows

Réunion du 13 novembre 2006



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 9 octobre 2006)

- Septembre 2006
  - MS06-056 Cross-site scripting via ASP.NET
    - Affecte : .NET Framework 2.0
    - Exploit : "cross-site scripting" via AutoPostBack
    - Crédit : Jaswinder Hayre / EY
  - MS06-057 Vulnérabilité dans le shell Windows
    - Affecte : Windows toutes versions supportées
    - Exploit : vulnérabilité déjà connue du contrôle ActiveX "WebViewFolderIcon" (fonction setSlice)
    - Crédit : N/D (historiquement, H. D. Moore)

Dernières vulnérabilités
Avis Microsoft (2/8)

- **MS06-058 Vulnérabilités multiples dans PowerPoint (x4)**
  - **Affecte : PowerPoint toutes versions supportées (y compris Mac)**
  - **Exploit : déjà exploitées dans la nature …**
  - **Crédit : Arnaud Dovi *via* ZDI, Dejun Meng / Fortinet, Chris Ries / VigilantMinds**

- **MS06-059 Vulnérabilités multiples dans Excel (x4)**
  - **Affecte : Excel toutes versions supportées (y compris Mac & Works)**
  - **Exploit : PoC disponible**
  - **Crédit : Manuel Santamarina Suarez *via* ZDI, NSFocus**

- **MS06-060 Vulnérabilités multiples dans Word (x4)**
  - **Affecte : Word toutes versions supportées (y compris Mac & Works)**
  - **Exploit : PoC disponible**
  - **Crédit : Chen Xiaobo / McAfee Avert Labs, Cu Fang**

Dernières vulnérabilités
Avis Microsoft (3/8)

- **MS06-061 Problème dans MSXML**
  - **Affecte : Windows toutes versions supportées, Office 2003 SP1/SP2**
  - **Exploit :**
    - **Violation de la politique de sécurité cross-domain**
    - **"Buffer overflow" dans le parser XSLT**
  - **Crédit : N/D**

- **MS06-062 Vulnérabilités multiples dans Office (x3)**
  - **Affecte : Office, Project, Visio toutes versions supportées (y compris Mac)**
  - **Exploit : exécution de code multiples**
  - **Crédit : Dejun Meng / Fortinet, Arnaud Dovi *via* ZDI, Sowhat / Nevis**

- **MS06-063 Déni de service dans le service Serveur**
  - **Affecte : Windows toutes versions supportées**
  - **Exploit :**
    - **DoS similaire à MS06-040**
    - **"Double free()" dans le noyau**
  - **Crédit : Gerardo Richarte / Core SDI, Matthew Amdur / VMWare, Fortinet, NSFocus**

Dernières vulnérabilités
Avis Microsoft (4/8)

- **MS06-064 Déni de service dans la pile IPv6**
  - **Affecte : Windows XP/2003 toutes versions supportées**
  - **Exploit : failles "TCP reset" et "ICMP reset" bien connues en IPv4**
  - **Crédit : N/D**

- **MS06-065 Exécution de code via "Object Packer"**
  - **Affecte : Windows XP/2003 toutes versions supportées**
  - **Exploit : problème dans *packager.exe* permettant l'exécution de code (avec interaction utilisateur)**
  - **Crédit : Andreas Sandblad / Secunia**

Dernières vulnérabilités
Avis Microsoft (5/8)

- **Bulletins du mois de novembre**
  - **1 bulletin MSXML, "critique" (Q927892 ?)**
  - **5 bulletins Windows, allant jusqu'à "critique"**
  - **Pas de bulletin Office**

Dernières vulnérabilités
Avis Microsoft (6/8)

EADS CCR

- **Révisions**
  - **MS06-038 Vulnérabilités Office**
    - **Version 1.5 : corrections sur l'installation administrative**
  - **MS06-042 Patch cumulatif pour IE**
    - **Version 2.1 : problème de compatibilité avec les scripts IE**
  - **MS06-048 Vulnérabilités Office**
    - **Version 1.1 : corrections sur la version Office pour Mac OS**
    - **Version 1.2 : *idem***
  - **MS06-055 Vulnérabilité "VML"**
    - **Version 1.1 : problèmes d'ACL sur VGX.DLL**
  - **MS06-056 Vulnérabilité dans ASP.NET 2.0**
    - **Version 1.1 : corrections sur les problèmes fréquemment rencontrés**
    - **Version 1.2 : Windows 2003 pour Itanium n'est pas affecté**

Dernières vulnérabilités
Avis Microsoft (7/8)

EADS CCR

- **Révisions (suite)**

  - **MS06-060 Vulnérabilité Word**
    - **Version 1.1 : corrections sur Word Viewer 2003**
  - **MS06-061 Vulnérabilité MSXML**
    - **Version 2.0 : meilleur support des versions 2.6, 4.0 et 6.0**
    - **Version 2.1 : précisions sur la distribution administrative**
  - **MS06-062 Vulnérabilités Office**
    - **Version 1.1 : précisions sur l'installation**
  - **MS06-063 Déni de service *via* le service Serveur**
    - **Version 1.1 : la faille ne peut pas être exploitée via le port TCP/593**

Dernières vulnérabilités
Avis Microsoft (8/8)

- Advisories

  - Q926043 -> MS06-057
  - Q925984 -> MS06-058
  - Q925059 -> MS06-060

  - Q917021 Modification du comportement du driver WiFi en WPA2
    - Plus d'association aux réseaux inconnus

  - Q927709
    - Vulnérabilité dans le contrôle ActiveX "WMI Object Broker" (Visual Studio 2005)
    - Pourtant connu depuis longtemps
      - http://metasploit.com/projects/Framework/exploits.html#ie_createobject

  - Q927892
    - Vulnérabilité MSXML 4.0 (une autre …)

Dernières vulnérabilités Infos Microsoft (1/3)

- Internet Explorer 7
  - Version finale disponible en anglais
    - Poussée automatiquement le 1er novembre 2006
    - Version française disponible quelques jours plus tard
  - Plateformes supportées :
    - Windows XP SP2 et Windows 2003 SP1
    - Windows XP et 2003 64 bits
  - La course aux failles ☺
    - http://secunia.com/Internet_Explorer_Arbitrary_Content_Disclosure_Vulnerability_Test/
    - http://secunia.com/internet_explorer_7_popup_address_bar_spoofing_test/
    - http://secunia.com/multiple_browsers_window_injection_vulnerability_test/
    - http://www.securitylab.ru/vulnerability/276342.php
    - http://aviv.raffon.net/2006/11/01/InternetExplorer7StillSpywareWritersHeaven.aspx
  - Pour être honnête, FireFox 2 n'est pas mieux loti ☺

Dernières vulnérabilités
Infos Microsoft (2/3)

- Interopérabilité NAP/NAC (Microsoft/Cisco)
  - http://download.microsoft.com/download/d/0/8/d08df717-d752-4fa2-a77a-ab29f0b29266/NAC-NAP_Whitepaper.pdf
- Microsoft CodePlex : le SourceForge du .NET
  - http://www.codeplex.com/
- Beta et RC
  - System Center Essentials 2007 Beta2
  - Visual Studio 2005 SP1 Beta
    - Permet de générer des exécutables relogeables (Vista)
    - http://blogs.msdn.com/michael_howard/archive/2006/09/26/772954.aspx
- Fin du support Windows XP SP1 depuis le 10 octobre 2006
- Le FBI remercie Microsoft pour sa participation à l'arrestation des auteurs de Mytob/Zotob
  - http://www.first.org/newsroom/globalsecurity/53050.html

Dernières vulnérabilités
Infos Microsoft (3/3)

- "Les 12 principes" de Microsoft pour entretenir la compétition
  - http://www.microsoft.com/presspass/newsroom/winxp/windowsprinciples.mspx
- Plus les choses changent …
  - http://www.live.com/?%3Ci%3E
- Faille PowerPoint publiée dans la nature
  - Non exploitable pour exécuter du code
  - Microsoft n'a jamais donné autant de détails techniques sur une faille
    - http://blogs.technet.com/msrc/archive/2006/11/10/follow-up-information-on-weblog-posting-about-poc-published-for-ms-office-2003-powerpoint.aspx

Dernières vulnérabilités
Autres avis (1/9) – failles

- "Vulnérabilité" Flash Player
  - Affecte : toutes versions jusqu'à la 9.0.16
  - Exploit :
    - Il est possible de modifier les entêtes HTTP via la méthode addRequestHeader()
    - Ceci permet de contourner les restrictions de la méthode send()
- Autre "vulnérabilité"
  - Affecte : Flash Player 9 / ActionScript 3
  - Exploitation : la fonction socket() a été introduite
- D'après Adobe, Flash équipe 97.3% des PCs dans le monde
  - A lire :
    - http://www.adobe.com/devnet/flashplayer/articles/flash_player_9_security.pdf
- 101 patches Oracle ce trimestre …
  - http://www.databasesecurity.com/oracle/OracleOct2006-CPU-Analysis.pdf

Dernières vulnérabilités
Autres avis (2/9) – failles

- "0day" dans Internet Explorer
  - http://isc.sans.org/diary.php?storyid=1807
  - Exploit : ActiveX "ADODB.Connection.2.7"

- MS06-042 ne corrige pas tous les problèmes avec les ActiveX
  - http://aviv.raffon.net/2006/08/14/MS06042OneSilentFixOneNoFix.aspx

- "0day" dans ICS (Internet Connexion Sharing)
  - Déni de service réalisable depuis le réseau interne uniquement
  - "Pointeur NULL" : pas d'exploitation en vue

  - Exploit (en Scapy) :
    - IP(dst="ics") / UDP() / DNS(rd=1, qdcount=0, qd=DNSQR(qname="www.google.com"))

Dernières vulnérabilités
Autres avis (3/9) – virus et spywares

- La police anglaise prévient 3000 personnes que leur PC a été piraté
  - http://weblog.infoworld.com/techwatch/archives/008319.html
  - Basé sur la fuite d'informations personnelles
- Defcon14 : "La mafia est en train de gagner la guerre du Net"
  - http://www.news.com.au/couriermail/story/0,23739,20042617-5003418,00.html
- Une base de données "temps réel" des *phishing*
  - http://phishery.internetdefence.net/
- Encore de la lutte anti-*phishing*
  - http://www.phishtank.com/
- WebAttacker : un toolkit "tout en un" pour $50 - $300
  - http://www.inet-lux.com/
  - http://www.websense.com/securitylabs/blog/blog.php?BlogID=94

Dernières vulnérabilités
Autres avis (4/9) – virus et spywares

- **Wikipedia pour héberger du Malware …**
  - **http://www.avertlabs.com/research/blog/?p=128**

- **Ainsi que YouTube (*via* une licence WMV)**
  - **http://www.websense.com/securitylabs/alerts/alert.php?AlertID=689**

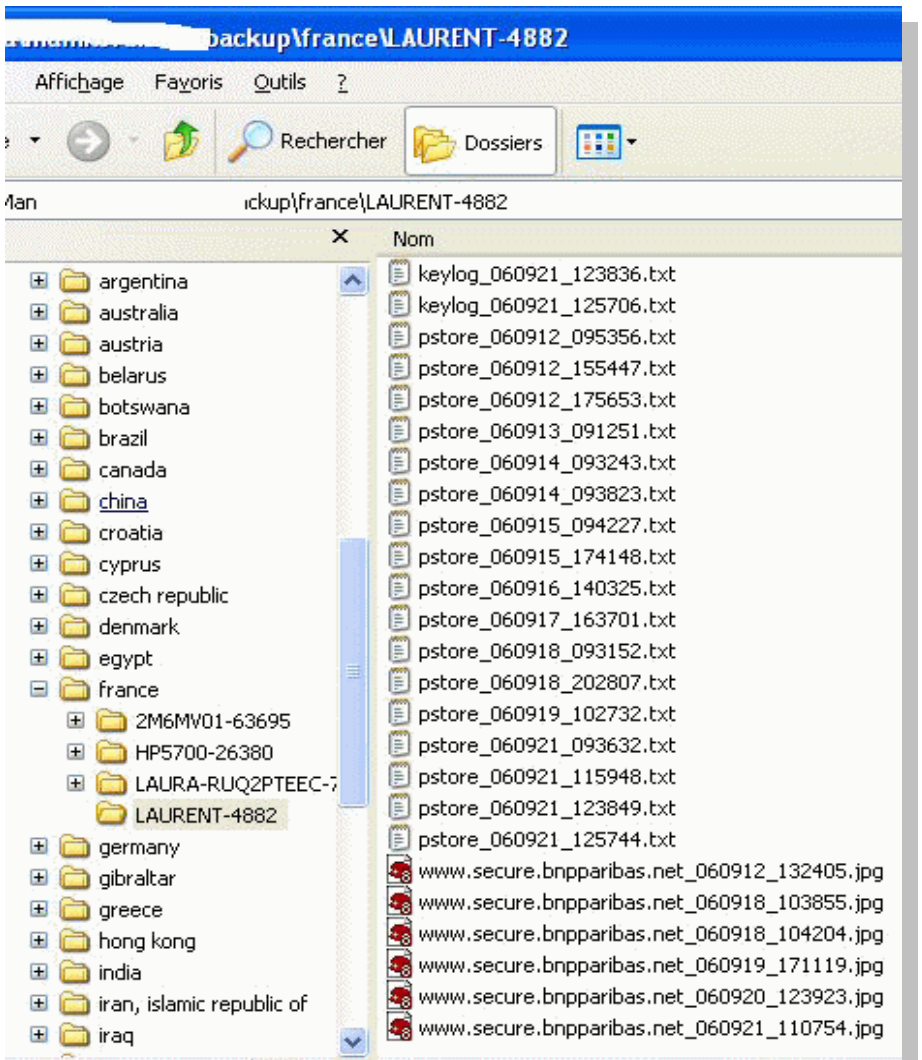
- **Le Top 10 des spammeurs**
  - **http://www.sophos.com/pressoffice/news/articles/2006/11/dirtydozq306.html**
    1. **United States 21.6%**
    2. **China (incl Hong Kong) 13.4%**
    3. **France 6.3%**
    4. **South Korea 6.3%**
    5. **Spain 5.8%**
    6. **Poland 4.8%**
    7. **Brazil 4.7%**
    8. **Italy 4.3%**
    9. **Germany 3.0%**
    10. **Taiwan 2.0%**
    11. **Israel 1.8%**
    12. **Japan 1.7%**

Dernières vulnérabilités
Autres avis (5/9) – virus et spywares

- Chercher des *malwares* courants avec Google
  - Tout a commencé par "signature:00004550"
  - Puis :
    - http://www.signature00004550.com/
    - http://metasploit.com/research/misc/mwsearch/

- Des virus créatifs
  - W32/Backdoor-DJC : communication par SMS
  - Troj/SpamThru : utilise son propre protocole de P2P
    - http://www.secureworks.com/analysis/spamthru/
    - Installe une version pirate de Kaspersky Antivirus pour éliminer tous les concurrents !
  - Un bot en Java
    - http://isc.sans.org/diary.php?storyid=1783
    - Une simple applet non signée qui demande les droits maximum sur le système

Dernières vulnérabilités
Autres avis (6/9) – virus et spywares



- **Vol d'identité : 4 victimes en France**
- **Les données envoyées sont bien souvent accessibles par toute personne qui analyse le virus**
- **(Source : McAfee Avert Labs)**

Dernières vulnérabilités
Autres avis (7/9)

- De nombreux sites Français "défacés" suite à l'adoption de la loi sur le génocide Arménien
  - Cf. Zone-h.org
- Une attaque contre Google ?
  - "Host Overflow Application eXception"
  - http://www.symantec.com/enterprise/security_response/weblog/2006/10/host_overflow_application_exce.html
  - ☺

Dernières vulnérabilités
Autres avis (8/9)

- "Google Code Search" déchaîne les passions
  - Chercher des failles
    - http://portal.spidynamics.com/blogs/msutton/archive/2006/10/06/Fun-With-Google-Code-Search.aspx
  - Chercher des failles … automatiquement !
    - http://www.cipher.org.uk/index.php?p=projects/bugle.project
  - Statistiques sur les failles triviales
    - http://monkey.org/~jose/blog/viewpage.php?page=google_code_search_stats
  - Et toujours plus de fun …
    - http://blogs.securiteam.com/index.php/archives/663
    - http://www.google.com/codesearch?q=kill+me+now&btnG=Search+Code
    - http://www.google.com/codesearch?q=%22go+to+hell%22&btnG=Search+Code
    - http://www.google.com/codesearch?q=+%22backdoor+password

Dernières vulnérabilités
Autres avis (9/9)

- La guerre autour de PatchGuard
  - La position de Microsoft
    - http://www.microsoft.com/security/windowsvista/allchin.mspx
  - Les contre : position de Symantec et McAfee
    - http://www.mcafee.com/us/local_content/misc/vista_position.pdf
  - Les pour : Sophos, Trend, Grisoft, Kaspersky, CA, F-Secure, …
    - http://www.sophos.com/pressoffice/news/articles/2006/10/vista-admins.html
  - Microsoft a des armes contre Symantec
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=417
  - Une API sera disponible dans le SP1 de Vista ?
    - http://www.darkreading.com/document.asp?doc_id=107498&WT.svl=cmpnews1_1
  - La société Authentium annonce vendre une technologie pour contourner PatchGuard
    - http://www.authentium.com/
    - Technologie VirtualATM : permet d'interagir avec le noyau sans lever d'exception
- Intel et Symantec travaille de leur côté sur un antivirus "de firmware"
  - http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=infrastructure&articleId=9003760&taxonomyId=14

Questions / réponses

- Questions / réponses
- Date de la prochaine réunion
  - Prochaine réunion le 11 décembre 2006
- N'hésitez pas à proposer des sujets et des salles