OSSIR
Groupe Sécurité Windows

Réunion du 11 septembre 2006

Revue des dernières vulnérabilités Microsoft

Cette veille est réalisée par les coanimateurs du groupe Windows

EdelWeb

Olivier REVENU
EdelWeb
olivier.revenu@edelweb.fr

Nicolas RUFF
EADS-CCR
nicolas.ruff@eads.net

Dernières vulnérabilités
Avis Microsoft (1/15)

- **Préalable**
  - **La criticité indiquée pour chaque avis est donnée selon l'échelle Microsoft, à savoir**

    Faible
    - **Une vulnérabilité dont l'exploitation est très difficile ou dont l'impact est minimale**

    Modéré
    - **L'exploitabilité est limitée par des facteurs comme la configuration par défaut non vulnérable ou est très difficile à réaliser**

    Important
    - **Une vulnérabilité dont l'exploitation aura pour impact l'atteinte à la confidentialité, l'intégrité ou la disponibilité des données des utilisateurs, voir l'intégrité ou la disponibilité du système**

    Critique
    - **Une vulnérabilité dont l'exploitation peut permettre la propagation d'un vers Internet sans action de l'utilisateur**

  - **Les exploits indiqués pour chaque avis sont ceux connus publiquement à la date de cette présentation**

Dernières vulnérabilités
Avis Microsoft (2/15)

- **Correctifs de Juillet 2006**
  - **4 bulletins Windows dont 2 de niveau « critique »**
  - **3 bulletins Office de niveau « critique »**

Bulletin	Faille	Affecte	Détails	Exploit
MS06-033	Fuite d'information via ASP.NET (Urs Eichmann)	framework .NET 2.0	Mauvaise gestion d'URLs malformées ➔ Accès à des zones non autorisées du site web	non
MS06-034	"Buffer overflow" dans le traitement des pages ASP (Brett Moore)	IIS 5.0, 5.1, 6.0	L'attaquant doit pouvoir uploader un fichier ASP ➔ Exécution de code sous IWAM_account	oui

Dernières vulnérabilités
Avis Microsoft (3/15)

Bulletin	Faille	Affecte	Détails	Exploit
MS06-035	**Vulnérabilités multiples dans le service "serveur"** (Pedram Amini, Nicolas Pouvesle, Mike Price, Rafal Wojtczuk)	**Windows toutes versions supportées**	**• "Memory leak" • "Heap overflow" exploitable via les mailslots RPC • Authentification requise sur les Windows récents ➔ Exécution de code sous SYSTEM**	**oui**
MS06-036	**"Buffer overflow" dans le client DHCP** (Mariano Nuñez Di Croce)	**Windows toutes versions supportées**	**Réponse DHCP malformée ➔ Exécution de code sous SYSTEM**	**oui**
MS06-037	**Vulnérabilités multiples dans Excel** (Posidron, NSFocus Security Team, Arnaud Dovi, iDEFENSE, Sowhat, Xin Ouyang, Shaun Colley, Costin Ionescu)	**Excel 2000 / XP / 2003 / Mac**	**8 failles corrigées ! (dont des failles "0day") ➔ Exécution de code dans le contexte de l'utilisateur**	**Partiel 0day**

Dernières vulnérabilités
Avis Microsoft (4/15)

Bulletin	Faille	Affecte	Détails	Exploit
MS06-038	**Failles Office multiples** (Elia Florio)	**Office 2000 / XP / 2003 / Mac / Project / Visio / Works**	**3 failles corrigées exploitables via un document Office malformé ➔ Exécution de code dans le contexte de l'utilisateur**	**non**
MS06-039	**Vulnérabilité dans les filtres Office** (Fortinet, NSFocus Security Team)	**Office 2000 / XP / 2003 / Project / Works**	**2 failles corrigées exploitables via des images PNG / GIF malformées ➔ Exécution de code dans le contexte de l'utilisateur**	**non**

Dernières vulnérabilités
Avis Microsoft (5/15)

- **Correctifs de août 2006**
  - **10 bulletins Windows allant jusqu'à "Critique"**
  - **2 bulletins Office allant jusqu'à "Critique"**

Bulletin	Faille	Affecte	Détails	Exploit
MS06-040	**Vulnérabilité dans le service "Serveur"** (US-CERT, SANS)	**Windows toutes versions supportées**	**"buffer overflow" Unicode Facilement exploitable sauf sous XP SP2 / W2K3 SP1 ➔ Exécution de code sous SYSTEM**	**0day + malware CME-482 CME-762**
MS06-041	**Vulnérabilités multiples dans la résolution DNS** (Peter Winter Smith - NGS Software, Mark Dowd -ISS X-Force)	**Windows toutes versions supportées**	**DNS Client, Winsock "hostname()" via une réponse DNS malformée ➔ Exécution de code sous SYSTEM**	**non**

Dernières vulnérabilités
Avis Microsoft (6/15)

Bulletin	Faille	Affecte	Détails	Exploit
MS06-042	**Mise à jour cumulative pour Internet Explorer** (Sam Thomas - TippingPoint / ZDI, Cody Pierce – TippingPoint, Will Dormann – CERT / CCElia Florio)	**IE toutes versions supportées**	•Redirect Cross-Domain Information Disclosure Vulnerability - CVE-2006-3280 •HTML Layout and Positioning Memory Corruption Vulnerability - CVE-2006-3450 •CSS Memory Corruption Vulnerability - CVE-2006-3451 •HTML Rendering Memory Corruption Vulnerability - CVE-2006-3637 •COM Object Instantiation Memory Corruption Vulnerability - CVE-2006-3638 •Source Element Cross-Domain Vulnerability - CVE-2006-3639 •Window Location Information Disclosure Vulnerability - CVE-2006-3640 •FTP Server Command Injection Vulnerability - CVE-2004-1166 (!) •Ex:ftp://ftp.example.com/%0aPORT%20a,b,c,d,e,f%0aRETR%20/file	**partiel**

Dernières vulnérabilités
Avis Microsoft (7/15)

Bulletin	Faille	Affecte	Détails	Exploit
MS06-043	Vulnérabilité dans Outlook Express	OE6 sous Windows XP / 2003	Exécution de code via un lien MHTML:// malformé ➔ Exécution de code dans le contexte de l'utilisateur	oui
MS06-044	"Cross-site scripting" dans la MMC (Yorick Koster - ITsec, HDM, Tom Gilder)	MMC sous Windows 2000 SP4	Accès à des ressources HTML dans la MMC, permettant l'exécution de commandes en zone locale Exploitable via une pièce jointe ou une page Web "res://mmcndmgr.dll/prevsym12.htm#%29%3B%3C/style%3E%3Cscript%20language…" http://browserfun.blogspot.com/2006/08/ms06-044-internet-explorer-5x.html	oui

Dernières vulnérabilités
Avis Microsoft (8/15)

Bulletin	Faille	Affecte	Détails	Exploit
MS06-045	Vulnérabilité dans EXPLORER	Windows toutes versions supportées	Dépôt de fichier à un emplacement arbitraire Requière une action "drag and drop" de l'utilisateur ➔ Exécution de code dans le contexte de l'utilisateur	oui
MS06-046	Vulnérabilité dans l'aide HTML (Cody Pierce - TippingPoint)	Windows toutes versions supportées	"buffer overflow" dans le composant ActiveX ➔ Exécution de code dans le contexte de l'utilisateur	oui
MS06-047	Vulnérabilité dans VBA (Ka Chun Leung - Symantec)	Office 2000 / XP, Works 2004 / 2005 / 2006	Exécution de code via des propriétés de document malformées	0day malware Mdropper

Dernières vulnérabilités
Avis Microsoft (9/15)

Bulletin	Faille	Affecte	Détails	Exploit
MS06-048	**Vulnérabilités dans PowerPoint** (Elia Florio -Symantec, Dejun Meng - Fortinet, Shih-hao Weng - ICSTC, SoWhat - Nevis Labs)	**Office 2000 / XP / 2003, Office 2004 / vX pour Mac**	**2 failles** • **Faille dans "mso.dll"** • **Enregistrement malformé** ➔ **Exécution de code dans le contexte de l'utilisateur**	**0day**
MS06-049	**Vulnérabilité dans le noyau** (Cody Pierce - TippingPoint)	**Windows 2000 SP4**	**Elévation de privilège en local** ➔ **Exécution de code sous SYSTEM**	**non**
MS06-050	**Vulnérabilités dans Hyperlink Object Library** (Pedram Amini - TippingPoint, Steve Tai - CSC Australia)	**Windows (toutes versions supportées)**	**2 vulnérabilités exploitables dans HHCTRL.OCX**	**0day**

Dernières vulnérabilités
Avis Microsoft (10/15)

Bulletin	Faille	Affecte	Détails	Exploit
MS06-051	**Vulnérabilités dans le noyau** (Reed Arvin - Canaudit, Matt Miller - Leviathan Security Group)	**Windows toutes versions supportées**	**2 failles** **• Elévation de privilège en local (Winlogon et DLL)** **• Exécution de code, possible via la visite d'un site web (traitement des exceptions)**	**non**

Dernières vulnérabilités
Avis Microsoft (11/15) - Synthèse

IMPACT MS	VECTEUR D'EXPLOITATION PREMIER Internet	LAN	Utilisateur
Exécution de code à distance	IIS (034)	SMB (035) DHCP (036) SRV (040) DNSClient (041)	OFFICE (037 / 038 / 039 / 047 / 048) OE (043) MMC (044) EXPLORER (045) HELP (046) HLINK (050) KERNEL (051) IE (042)
Élévation de privilèges			KERNEL (049) KERNEL (051)
Usurpation de contenu			
Déni de service			
Divulgation d'informations	.NET 2 (33)	SMB (035)	IE (042)

Dernières vulnérabilités
Avis Microsoft (12/15)

- **Prochain bulletins de septembre 2006**
  - **2 bulletins Windows de niveau allant jusqu'à un niveau "important"**
  - **1 bulletin Office de niveau "critique"**
  - **mise à jour de l'outil MSRT**

Dernières vulnérabilités
Avis Microsoft (13/15)

- Advisories
  - Q922437 : code d'exploitation pour MS06-040
  - Q922970 : « 0day » PowerPoint 2000 / XP / 2003
    - Corrigé par MS06-048
  - Q923762 : le patch MS06-042 introduit une nouvelle faille !
  - Q925059 : « 0day » Word 2000 (CVE-2006-4534)

Dernières vulnérabilités
Avis Microsoft (14/15)

- Révisions
  - MS06-024
    - Version 1.3 : mise à jour des clés de base de registre
  - MS06-027
    - Version 1.3 : précisions sur les bulletins remplacés
  - MS06-033
    - Version 1.2 : mise à jour des "caveats" et des prérequis
  - MS06-034
    - Version 1.1 : clarifications
    - Version 1.2 : gros problèmes de détection sur Windows 2003 SP1
  - MS06-035
    - Version 1.1 : bulletin publié
  - MS06-037
    - Version 1.1 : clarifications
  - MS06-038
    - Version 1.1 : clarifications
    - Version 1.2 : mise à jour de la liste des fichiers remplacés
  - MS06-039
    - Version 1.1 : clarifications

Dernières vulnérabilités
Avis Microsoft (15/15)

- Révisions
  - MS06-040
    - Version 1.1
      - Incompatibilité avec les applications qui allouent plus de 1 Go de mémoire
        - Ex. Microsoft Navision 3.7
      - Précision sur les ports à bloquer
  - MS06-042
    - Version 1.2
      - Incompatibilités avec les applications PeopleSoft
        - http://support.microsoft.com/kb/923762/en-us
        - Problème avec HTTP/1.1 et la compression
        - Ce problème est exploitable ! (Q923762)
    - Version 2.0
      - Le patch d'origine introduisait un nouveau bogue de type "buffer overflow" !

Dernières vulnérabilités
Infos Microsoft (1/3)

- Virtual PC est gratuit
  - Virtual PC 2007 supportera Vista
- Open Document Format vs. Open XML Format
  - Microsoft publie un outil de conversion
  - http://sourceforge.net/projects/odf-converter
- Microsoft publie "Private Folders 1.0"
  - Critiqué et retiré une semaine après sa sortie
    - http://news.com.com/Microsoft+shutters+Windows+private+folders/2100-1012_3-6094481.html
  - Nécessite Windows XP SP2 et WGA installé pour le télécharger
- Microsoft rachète Sysinternals / Winternals
- "Strider URL Tracer with Typo-Patrol"
  - http://research.microsoft.com/URLTracer/

Dernières vulnérabilités
Infos Microsoft (2/3)

- Les sociétés retenues pour auditer Vista
  - http://blogs.msdn.com/windowsvistasecurity/archive/2006/07/28/681833.aspx
- Microsoft acquiert Whale Communications
  - Un futur VPN-SSL dans ISA Server …
- Actualité des patches
  - Microsoft distribuera IE 7 via Windows Update sous forme de mise à jour "haute priorité"
    - http://news.com.com/Microsoft+tags+IE+7+high+priority+update/2100-7350_3-6098500.html?tag=nefd.lede
  - 100 millions de téléchargement en 30h pour le patch MS06-040
    - Belle performance technique
  - MS06-035 pas totalement patché ?
    - Juste un DoS pour le moment
    - http://blogs.technet.com/msrc/archive/2006/07/28/443837.aspx
  - MDAC 2.7 "Service Pack 1 Refresh"
    - En fait un nouveau SP1 avec plus de correctifs ☺

Dernières vulnérabilités
Infos Microsoft (3/3)

- Alphas, Betas et CTP
  - Internet Explorer 7 RC1
  - Windows Desktop Search 3.0 Beta2
  - Windows Media Player 11 Beta
  - .NET Framework 3.0 CTP

Dernières vulnérabilités
Autres avis (1/12) – failles

- Synthèse des patchs MS avec problèmes et exploits connus
  - http://isc.sans.org/diary.php?storyid=1611

- Black Hat US 2006 : une conférence à grand spectacle
  - « BluePill » : démonstration d'une faille de conception dans les processeurs AMD avec les extensions SVM
  - Faille exploitable dans les drivers WiFi Centrino < 9.4.0.7
  - Faille exploitable dans certains drivers WiFi pour Mac
    - http://news.com.com/Flawed+Wi-Fi+drivers+can+expose+PCs/1606-2_3-6101573.html?tag=fd_cars

- Defcon 14
  - Malware pour Windows Mobile 4.2 se propageant via MMS
    - Exploite un "buffer overflow" dans le parser SMIL
      - http://www.avertlabs.com/research/blog/?p=64

Dernières vulnérabilités
Autres avis (2/12) – failles

- "0day" Word
  - Non exploitable d'après MSRC
- "0day"(s) PowerPoint
  - Corrigé par MS06-048
    - Encore un coup des chinois ☺
      - http://isc.sans.org/diary.php?storyid=1484
    - Voir aussi :
      - http://blogs.securiteam.com/?p=508
  - Un autre non corrigé ?
    - http://isc.sans.org/diary.php?storyid=1621
  - A priori non
    - http://blogs.technet.com/msrc/archive/2006/08/23/449075.aspx
- "0day" Works
  - http://www.securityfocus.com/archive/1/440056

Dernières vulnérabilités
Autres avis (3/12) – failles

- Faille Flash Player
  - Affecte : Flash Player 8.0.24.0 (passer à Flash Player 9)
  - Exploit : failles multiples
  - Crédit : Dejun Meng (Fortinet)

- Faille dans GDIPLUS.DLL
  - Affecte : Windows (toutes versions supportées)
  - Exploit :
    - http://seclists.org/bugtraq/2006/Jul/0538.html
    - Exploitabilité douteuse (déni de service)

- Déni de service dans RRAS
  - Affecte : patch MS06-025 incomplet ?
  - Exploit :
    - Disponible dans Metasploit 3.0
    - http://www.metasploit.com/archive/framework/msg01110.html
  - Crédit : HDM

Dernières vulnérabilités
Autres avis (4/12) – failles

- 65 failles corrigées par Oracle en juillet 2006
  - Pas de détails sans login
  - Aucun "workaround"
- Mise à jour Firefox 1.5.0.5
  - Corrige 12 failles dont 7 critiques
- Mise à jour Firefox 1.5.0.6 (quelques jours plus tard)
  - Un simple problème de compatibilité avec les liens "mms://"

Dernières vulnérabilités
Autres avis (5/12) – failles IE

- Un moteur de recherche de malware par HD Moore
  - http://metasploit.com/research/misc/mwsearch/index.html
- Une application d'analyse des malwares sous VMWare
  - http://www.consolo.de/html/cwsandbox.asp
- La saga du "bug of the day"
  - Beaucoup de DoS
  - Quelques bugs exploitables
    - http://browserfun.blogspot.com/2006/07/mobb-18-webviewfoldericon-setslice.html
- Les bogues de type "NULL pointer" sont exploitables dans Internet Explorer !
  - http://uninformed.org/?v=4&a=5&t=sumry
- Les attaques AJAX/JavaScript font couler beaucoup d'encre …
  - http://www.zdnet.com.au/news/security/soa/JavaScript_opens_doors_to_browser_based_attacks/0,2000061744,39265130,00.htm
  - Rien de très nouveau

Dernières vulnérabilités
Autres avis (6/12) – virus et spywares

- W32/Gatt : le premier virus anti-IDA Pro !
- Mobler : un virus Windows + Symbian
- FormSpy : un spyware sous forme de plugin FireFox
  - Fichier .xpi
  - Se copie directement dans le répertoire (pas de confirmation)
  - Surveille clavier et souris
- WmvDownloader-* utilisent le système de DRM Windows Media pour télécharger du malware
  - http://www.theregister.co.uk/2005/01/13/drm_trojan/
- Une publicité sur MySpace infecte 1 million d'utilisateurs
  - http://www.techspot.com/news/22309-myspace-banner-ad-infects-millions-of-windows-users-with-spyware.html
  - Utilisation de la faille WMF
- MSH/Cibyz
  - Un autre virus "proof-of-concept" pour Windows Powershell
  - Virus existant précédemment : MSH/Danom

Dernières vulnérabilités
Autres avis (7/12) – virus et spywares

- Le premier virus en langage LUA
  - http://www.avertlabs.com/research/blog/?p=72
  - Affecte de nombreux MMORPG !
- Une signature de CA détecte LSASS.EXE comme "Win32/Lassrv.B"
- Un Cheval de Troie utilise de l'évasion ICMP
  - http://www.websense.com/securitylabs/alerts/alert.php?AlertID=570
- Les virus Symbian sont-ils légion ?
  - CA vs. F-Secure
    - http://news.zdnet.co.uk/internet/security/0,39020375,39279551,00.htm
  - F-Secure annonce la sortie de CommWarrior.Q
- Un "buffer overflow" …
  - … dans l'onglet "Buffer OverFlow Protection Properties" de McAfee 8.0.0
  - http://lists.grok.org.uk/pipermail/full-disclosure/2006-July/047753.html
- Phishing sur le site de BNP Paribas (UK)
  - http://www.websense.com/securitylabs/alerts/alert.php?AlertID=561

Dernières vulnérabilités
Autres avis (8/12) – virus et spywares

- Une nouvelle menace : le Smishing ☺
  - Phishing par SMS
- McAfee lance le magazine SAGE
  - 20 Mo en PDF …
  - Débat sur l'utilisation de CVS par les auteurs de virus
    - Certains en concluent que le logiciel libre est nocif !
  - De manière générale, une véritable attaque contre le logiciel libre …
- Peut-on faire confiance à l'industrie des antimalwares ?
  - http://software.newsforge.com/article.pl?sid=06/06/06/1832223
  - Réponse : non, car il est dans leur intérêt que les utilisateurs continuent à être attaqués par des virus ☺
- Pourquoi les antivirus les plus connus sont moins bons ?
  - http://www.zdnet.com.au/blogs/securifythis/soa/Why_popular_antivirus_apps_do_not_work_/0,39033341,39264249,00.htm
  - Parce que les auteurs de virus testent leurs créations sur ceux là

Dernières vulnérabilités
Autres infos (9/12)

- Les adolescents européens et la sécurité informatique
  - http://www.theitshield.com/pr/8750
- Un autre site d'intérêt pour les adolescents, bien que 100% Microsoft
  - http://www.decodeleweb.com/
- Une fuite qui fait du bruit
  - 19 million de recherches, faites par 658,000 clients AOL
  - http://data.aolsearchlogs.com/
- Intel licencie 1000 managers
  - http://news.com.com/Intel+to+ax+1,000+managers/2100-1014_3-6093843.html

Dernières vulnérabilités
Autres infos (10/12)

- "L'affaire WGA" : ça se durcit
  - Taux de piratage mesuré : 11,7%
  - "Windows Genuine Disadvantage"
    - http://www.theregister.co.uk/2006/07/07/wga_disadvantage/
    - Une "Class Action" lancée contre Microsoft
  - Q921914 : comment désinstaller WGA
  - Cuebot-K : se fait passer pour WGA
    - http://www.theregister.co.uk/2006/07/03/wga_worm/

- Symantec fait une revue de Vista
  - http://www.symantec.com/avcenter/reference/ATR-VistaAttackSurface.pdf
  - Où il est question de Teredo …
  - La pile IP a été réécrite "from scratch" !
    - http://www.osnews.com/story.php?news_id=15399

Dernières vulnérabilités
Autres infos (11/12)

- **DADVSI : le conseil constitutionnel tranche … et durcit la loi !**
  - **Plus d'exonération pénale pour les auteurs de logiciels de P2P**
  - **Plus d'exonération pénale pour l'analyse des DRM**
  - **Prison pour ceux qui téléchargent (et non plus amende)**

Dernières vulnérabilités
Autres infos (12/12)

- Et pendant ce temps là sur la mailing liste de l'OSSIR

  - Liste SUR
    - Il n'a de libre que le nom
    - Virtualisation et convergence

  - Liste NT
    - Une autre grenouille bleu va prendre la suite de BlueFrog
    - Collection de vieux logiciels vulnérables
    - Le protocole de Skype "cracké" ?

Questions / réponses

- Questions / réponses
- Date de la prochaine réunion
  - Prochaine réunion le 9 octobre 2006
- N'hésitez pas à proposer des sujets et des salles