# OSSIR
# Groupe Sécurité Windows

**Réunion du 11 décembre 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 (1/8)

- **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 (2/8)

- **Correctifs de Octobre 2006**
  - **bulletins Windows dont 2 de niveau « critique »**
  - **bulletins Office de niveau « critique »**

| Bulletin | Faille | Affecte | Détails | Exploit |
|---|---|---|---|---|
| MS06-066 | **Vulnérabilités multiples dans le client NetWare** (Peter Winter-Smith / NGS Software Sam Arun Raj / McAfee) | **Windows (toutes versions supportées sauf x64 et Vista)** | **"Heap Overflow", DoS via un paquet malformé** | **Oui (PoC)** |
| MS06-067 | **Patch cumulatif pour IE** (Sam Thomas / ZDI) | **IE toutes versions supportées (sauf IE 7)** | **Ancien "0day" dans DirectAnimation, "Heap Overflow"** | **Oui (en cours d'exploitation)** |

# Dernières vulnérabilités
# Avis Microsoft (3/8)

| Bulletin | Faille | Affecte | Détails | Exploit |
|---|---|---|---|---|
| MS06-068 | Faille dans Microsoft Agent (n/c) | Windows toutes versions supportées | "Buffer Overflow" via un fichier ".ACF" malformé (exploitable via ActiveX) | Non |
| MS06-069 | Vulnérabilités Flash Player multiples (Stuart Pearson / Computer Terrorism) | Flash Player 6 sur Windows XP SP2 | "Buffer Overflow" via fichier ".SWF" malformé, abus de droits, … | Non |
| MS06-070 | Vulnérabilité dans le service Workstation (eEye) | Windows 2000 SP4, Windows XP SP2 | Exploitation de code à distance | Oui |

# Dernières vulnérabilités
# Avis Microsoft (4/8)

| Bulletin | Faille | Affecte | Détails | Exploit |
|---|---|---|---|---|
| MS06-071 | **Vulnérabilités MSXML** (Robert Freeman / ISS Dror Shalev, Moti Jospeh / Checkpoint) | **MSXML 4.0, MSXML 6.0** | **exécution de code (remplace MS06-061)** | **Oui (0day)** |

- **Une bonne analyse des patches Microsoft**
  - **http://www.eeye.com/research/html/newsletters/alert/AL20061114.html**
  - **http://isc.sans.org/diary.php?date=2006-11-16**

# Dernières vulnérabilités
# Avis Microsoft (5/8) - Synthèse

| IMPACT MS | VECTEUR D'EXPLOITATION PREMIER<br>Internet | LAN | Utilisateur |
|---|---|---|---|
| **Exécution de code à distance** | | **NETWARE (066)**<br>**WORKSTATION (070)** | **IE (067)**<br>**MS AGENT (068)**<br>**FLASH (069)**<br>**MSXML (071)** |
| **Élévation de privilèges** | | | |
| **Usurpation de contenu** | | | |
| **Déni de service** | | | |
| **Divulgation d'informations** | | | |

# Dernières vulnérabilités
# Avis Microsoft (6/8)

- **Prochain bulletins de décembre 2006**
  - **5 bulletins Windows de niveau allant jusqu'à un niveau "critique"**
  - **1 bulletin Visual Studio de niveau "critique"**
  - **Mise à jour de l'outil MSRT**
  - **Pas de patch pour le(s) "0day" Word**

# Dernières vulnérabilités
# Avis Microsoft (7/8)

- **Advisories**
  - **Q925143 : MS06-069 (Flash)**
  - **Q925444 : MS06-067 (DirectAnimation ActiveX)**
  - **Q927892 : MS06-071 (MSXML)**
  - **Q928604**
    - **Code d'exploitation pour la faille Workstation (MS06-070)**
  - **Q929433**
    - **"0day" Word (toutes versions)**
    - **Note : une autre faille Word a été découverte par McAfee "in the wild"**

# Dernières vulnérabilités
# Avis Microsoft (8/8)

- **Révisions**
  - **MS06-012**
    - **Version 1.3 : mise à jour des patches remplacés**
  - **MS06-020 Vulnérabilité Flash Player**
    - **Version 1.1 : Windows XP 64 bits est affecté par cette faille**
  - **MS06-033**
    - **Version 1.3 : FAQ mis à jour**
  - **MS06-039**
    - **Version 1.2 : mise à jour des produits affectés**
  - **MS06-056**
    - **Version 1.3 : FAQ mis à jour**
  - **MS06-059**
    - **Version 1.1 : Excel Viewer 2003 est affecté**
  - **MS06-069 Vulnérabilité Flash Player**
    - **Version 1.1 : précisions sur Flash 6.0**
  - **MS06-071 Vulnérabilité MSXML**
    - **Version 1.1 : mise à jour du nom de fichier et du numéro de KB**

# Dernières vulnérabilités
# Infos Microsoft (1/2)

- **Le rapport du MSRT, période Janvier -> Juin 2006**
  - **Sources**
    - **MSRT : 290 millions de clients**
    - **Windows Defender : 14 millions de clients**
    - **OneCare version gratuite : 7 million de clients**
  - **Résultats**
    - **10 millions de malwares effacés**
    - **Les malwares les plus répandus sont les Bots, suivi par les Keyloggers**
    - **Dans 20% des cas un rootkit est présent**
    - **Le "rootkit" Sony est 9ème**

**http://www.microsoft.com/downloads/details.aspx?FamilyId=1C443104-5B3F-4C3A-868E-36A553FE2A02&displaylang=en**

# Dernières vulnérabilités
# Infos Microsoft (2/2)

- **Prolongation du support de SUS : 10 juillet 2007**
- **Microsoft se lance dans l'hébergement**
  - **http://office.microsoft.com/en-us/officelive/**
- **Microsoft lance IVA**
  - **Interoperability Vendor Alliance**
- **Microsoft les OEMs majeurs d'activer NX/XD par défaut**
  - **http://blogs.msdn.com/michael_howard/archive/2006/12/06/windows-vista-aslr-dep-and-oems.aspx**
- **Sorties**
  - **Windows Media Player 11**
  - **SharePoint 3.0**
  - **ForeFront (Beta publique)**
  - **RMS 1.0 SP2**
  - **Windows 2003 SP2 RC1**
  - **Utilitaires**
    - **Windows Automated Installation Kit (WAIK)**
    - **Anti-XSS Library 1.5**
    - **XML Notepad 2007**
    - **RDP Client 6.0**
    - **…**

# Dernières vulnérabilités
# Autres avis (1/12) – failles

- **Déni de service sur Active Directory**
  - **Affecte : Windows 2000 SP4**
  - **Exploit :**
    - **Mis en vente le jour du Patch Tuesday dans Gleg VulnDisco Pack**
    - **http://secunia.com/advisories/22871/**
    - **http://www.securityfocus.com/bid/21083/**

- **Faille(s) Acrobat 7.0.8**
  - **Découverte par FrSIRT, publiée et non patchée**
  - **http://www.frsirt.com/english/advisories/2006/4751**

- **Faille Adobe Download Manager <= 2.1**
  - **http://research.eeye.com/html/advisories/published/AD20061205.html**

- **Faille WinZip 10**
  - **Dans un contrôle ActiveX marqué "safe for scripting"**
  - **Désactivé par MS06-067**

# Dernières vulnérabilités
# Autres avis (2/12) – failles

- **Le "0day tracker" de eEye**
  - **Statistiques et informations sur les "0day" passés et présents**
  - **http://research.eeye.com/html/alerts/zeroday/index.html**

- **La semaine des failles Oracle**
  - **Annulé au dernier moment !**
  - **http://www.argeniss.com/woodb.html**

- **CRC32 pour protéger les mots de passe des PST**
  - **De nombreuses collisions**
  - **Exemple : eyzVS1 = tHPuT3 = 5J8j84 = *CRC null***
  - **http://www.nirsoft.net/articles/pst_password_bug.html**

# Dernières vulnérabilités
# Autres avis (3/12) – failles Web

- **Une liste de failles IE7 non patchées**
  - **http://home.doramail.com/fileserver/index.htm**
- **Georgi Guninski prend sa retraite ☺**
- **L'auteur du rootkit Hacker Defender serait mort dans un accident de voiture ☹**
  - **http://forum.sysinternals.com/forum_posts.asp?TID=8772**
- **Un nouveau type de faille**
  - **Reverse Cross-Site Request (RCSR)**
  - **Permet de récupérer les mots de passe mémorisés dans le navigateur (ex. Firefox 2.0)**
  - **http://www.info-svc.com/news/11-21-2006/**
- **Exploiter des failles Cross Site Request Forgery (CSRF) via Word ?**
  - **Utilisation des IFRAMEs dans un ".DOC"**
  - **http://forum.sysinternals.com/forum_posts.asp?TID=8772**

# Dernières vulnérabilités
# Autres avis (4/12) – virus et spywares

- **Virus créatifs**
  - **"W32/Realor.worm" cible les fichiers RealPlayer (*.rmvb)**
  - **"W32/Kibik.a"**
    - **Infecte Explorer.EXE (virus parasite)**
    - **Communique avec son maître via Google BlogSearch**
  - **Un virus de script en action dans SecondLife !**
    - **http://www.youtube.com/watch?v=5H8hNXWgOoE**
  - **Un trojan se protège avec EFS**
    - **http://www.avertlabs.com/research/blog/?p=77%E2%80%A2J2ME/Redbrowser**
  - **Un ver se propage sur MySpace à travers une vidéo QuickTime**
    - **http://www.websense.com/securitylabs/alerts/alert.php?AlertID=708**

- **De plus en plus de virus protégés contre l'analyse**
  - **3 sur 12 d'après le SANS**
  - **Utilisation de packers commerciaux avec détection de VMWare (ex. Themida)**
  - **http://isc.sans.org/diary.php?storyid=1871**

# Dernières vulnérabilités
# Autres avis (5/12) – virus et spywares

- **Contourner les antivirus par une erreur d'encodage MIME**
  - **http://www.quantenblog.net/security/virus-scanner-bypass**
- **TypoSquatting amusant**
  - **Avec l'ouverture du ".eu", il est facile de squatter le ".edu"**
  - **http://isc.sans.org/diary.php?storyid=1866**
- **Sur le front du spam**
  - **Double en volume tous les ans**
  - **+20 points sur les spams en image**
  - **819 TO par jour de bande passante**
  - **http://www.computerworld.com.au/index.php/id;441511209;fp;2;fpid;1**

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

- **Les antivirus se doivent de protéger contre les attaques ciblées**
  - **Analyse du Gartner Group**
  - **Sophos est précurseur avec la technologie "Genotype"**
  - **http://www.zdnet.com.au/news/security/soa/Antivirus_firms_target_unique_malware/0,130061744,339272340,00.htm**

- **Symantec : "les auteurs de malwares prennent des week-ends de 3 jours"**
  - **http://www.vnunet.com/vnunet/news/2169996/symantec-phishers-mondays**

- **Un livre en français**
  - **« Cybercriminalité, Enquête sur les mafias qui envahissent le web »**
  - **Eric Filiol (ESAT) et Philippe Richard (journaliste)**

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

- **Les "prédictions" de McAfee pour 2007**

1. **The number of password-stealing websites will increase using fake sign-in pages for popular online services such as eBay.**
2. **The volume of spam, particularly bandwidth-eating image spam, will continue to increase.**
3. **The popularity of video sharing on the web makes it inevitable that hackers will target MPEG files as a means to distribute malicious code.**
4. **Mobile phone attacks will become more prevalent as mobile devices become 'smarter' and more connected.**
5. **Adware will go mainstream following the increase in commercial Potentially Unwanted Programs.**

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

6. **Identity theft and data loss will continue to be a public issue – at the root of these crimes is often computer theft, loss of back-ups and compromised information systems.**

7. **The use of bots, computer programs that perform automated tasks, will increase as a tool favoured by hackers.**

8. **Parasitic malware, or viruses that modify existing files on a disk, will make a comeback.**

9. **The number of rootkits on 32-bit platforms will increase, but protection and remediation capabilities will increase as well.**

10. **Vulnerabilities will continue to cause concern fuelled by the underground market for vulnerabilities.**

# Dernières vulnérabilités
# Autres infos (9/12)

- **Le Top 20 SANS mis à jour**
  - **Operating Systems**
    - **W1. Internet Explorer**
    - **W2. Windows Libraries**
    - **W3. Microsoft Office**
    - **W4. Windows Services**
    - **W5. Windows Configuration Weaknesses**
    - **M1. Mac OS X**
    - **U1. UNIX Configuration Weaknesses**
  - **Cross-Platform Applications**
    - **C1 Web Applications**
    - **C2. Database Software**
    - **C3. P2P File Sharing Applications**
    - **C4 Instant Messaging**
    - **C5. Media Players**
    - **C6. DNS Servers**
    - **C7. Backup Software**
    - **C8. Security, Enterprise, and Directory Management Servers**

# Dernières vulnérabilités
# Autres infos (10/12)

- **Le Top 20 SANS mis à jour (suite)**
  - **Network Devices**
    - **N1. VoIP Servers and Phones**
    - **N2. Network and Other Devices Common Configuration Weaknesses**
  - **Security Policy and Personnel**
    - **H1. Excessive User Rights and Unauthorized Devices**
    - **H2. Users (Phishing/Spear Phishing)**
  - **Special Section**
    - **Z1. Zero Day Attacks and Prevention Strategies**

# Dernières vulnérabilités
# Autres infos (11/12)

- **La société TalkPlus a *reversé* le protocole Skype**
  - **http://www.talkplus.com/**
  - **http://www.skypejournal.com/blog/archives/2006/11/talkplus_demo_call_to_echo123_from_a_mob.php**
  - **http://www.skypejournal.com/blog/archives/2006/11/yes_talkplus_reverse_engineered_skype.php**

- **Le gouvernement anglais alerte les entreprises contre des attaques ciblées**
  - **http://www.computerweekly.com/Articles/2006/11/21/220089/Foreign+intelligence+agents+hacking+UK+businesses%2c+government.htm**
  - **Sources des attaques : Russie, Corée du Nord, Chine**

- **24 personnes ont travaillé sur le menu "éteindre" de Vista ☺**
  - **http://www.drizzle.com/~lettvin/2006/11/windows-shutdown-crapfest.html**

# Dernières vulnérabilités
# Autres infos (12/12)

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

  - **Liste SUR**
    - **Microsoft contre le reste du monde**
    - **Gestionnaire de mot de passe**
    - **Poste en libre service**
    - **Le Monde : la fin des échanges en ligne…**

  - **Liste NT**
    - **Générateur de trame libre**
    - **Client de calcul distribué de tables rainbow**

# Questions / réponses

- **Questions / réponses**
- **Date de la prochaine réunion**
  - **Prochaine réunion le 15 janvier 2007**
  - **AG le 16 janvier 2007**
- **N'hésitez pas à proposer des sujets et des salles**

**Joyeux Noël**