OSSIR
Groupe Sécurité Windows

Réunion du 12 novembre 2007

Revue des dernières vulnérabilités Microsoft

Cette veille est réalisée par les coanimateurs du groupe Windows

EdelWeb

Olivier REVENU
olivier.revenu (à) edelweb.fr

Mickaël DEWAELE
mickael.dewaele (à) edelweb.fr

Nicolas RUFF
EADS-IW
nicolas.ruff (à) eads.net

Dernières vulnérabilités
Avis Microsoft (1/7)

- **Correctifs de Octobre 2007**

  - **MS07-055 Vulnérabilité(s) dans "Kodak Image Viewer"**
    - **Affecte : Windows 2000 (et versions mises à jour de Windows)**
    - **Exploit : affecte (a priori) les formats JPEG et TIFF**
      - **CVE-2007-2217**
    - **Crédit : Cu Fang ; Rita Schappler / Global 360**

  - **MS07-056 Mise à jour cumulative pour Outlook Express**
    - **Affecte : Outlook Express et Windows Mail (toutes versions supportées)**
    - **Exploit : "heap overflow" lors de la connexion à un serveur NNTP**
      - **CVE-2007-3897**
    - **Crédit : iDefense**

Dernières vulnérabilités
Avis Microsoft (2/7)

- MS07-057 Mise à jour cumulative pour Internet Explorer
  - Affecte : Internet Explorer
  - Exploit :
    - CVE-2007-1091, CVE-2007-3826, CVE-2007-3892 : spoofing de la barre d'adresse
    - CVE-2007-3893 : exécution de code via une mauvaise gestion d'erreur
    - + nouveaux "kill bits"
  - Crédit : Pierre Geyer / next.motion OHG ; Carsten H. Eiram, Jakob Balle / Secunia Research

- MS07-058 Déni de service RPC
  - Affecte : Windows (toutes versions supportées)
  - Exploit : permet de tuer à distance n'importe quel service RPC
    - CVE-2007-2228
  - Crédit : ZDI

Dernières vulnérabilités
Avis Microsoft (3/7)

- **MS07-059 Vulnérabilité dans SharePoint**
  - **Affecte : SharePoint Server 3.0, Office SharePoint Server 2007**
  - **Exploit : publication de script sur le serveur (*cross-site scripting* ?)**
    - **CVE-2007-2581**
  - **Crédit : n/d**

- **MS07-060 Vulnérabilité dans Word**
  - **Affecte : Office 2000, Office XP, Office 2004 pour Mac**
  - **Exploit : exécution de code via un fichier Word malformé**
  - **Crédit : Liu Kun-Hao / Information and Communication Security Technology Center**

- **Notes :**
  - **Le 7ème bulletin prévu a disparu !**
  - **Une bonne analyse (technique) des patches d'octobre :**
    - **https://strikecenter.bpointsys.com/articles/2007/10/10/october-2007-microsoft-tuesday**

Dernières vulnérabilités
Avis Microsoft (4/7)

- **Prévisions pour Novembre 2007**
  - **1 avis critique affectant Windows XP et 2003**
    - **Impact : exécution de code à distance**
  - **1 avis important affectant Windows 2000 Server et 2003 Server**
    - **Impact : spoofing**

Dernières vulnérabilités
Avis Microsoft (5/7)

- Advisories

  - Q943521 : comportement de ShellExecute()
    - Affecte : IE 7 sur Windows XP SP2 et Windows 2003
    - Exploit : cf. "faille PDF" via l'URI "mailto:"
      - http://www.microsoft.com/technet/security/advisory/943521.mspx
      - http://blogs.technet.com/msrc/archive/2007/10/10/msrc-blog-additional-details-and-background-on-security-advisory-943521.aspx
      - http://blogs.msdn.com/ie/archive/2007/07/18/enriching-the-web-safely-how-to-create-application-protocol-handlers.aspx

  - Q944653 : faille dans le driver Macrovision
    - Cf. plus loin

Dernières vulnérabilités
Avis Microsoft (6/7)

- **Révisions**
  - **MS05-004 Faille ASP.NET**
    - **Version 4.0 : Windows 2003 SP2 et Vista sont affectés si le Framework .NET 1.0 ou 1.1 est installé**
  - **MS05-032**
    - **Version 2.2 : MS05-032 est remplacé par MS06-068 + MS07-045**
  - **MS06-006**
    - **Version 1.1 : effets de bord documentés dans Q937986**
  - **MS06-068**
    - **Version 1.2 : MS05-032 est remplacé par MS06-068 + MS07-045**
  - **MS07-027**
    - **Version 1.4 : répertoire manquant (IE 7 + Windows 2003)**
  - **MS07-045**
    - **Version 1.3 : mise à jour de la liste des fichiers affectés**

Dernières vulnérabilités
Avis Microsoft (7/7)

- Révisions (suite)
  - MS07-055
    - Version 1.1 : Windows XP 64 n'est pas affecté
  - MS07-056
    - Version 2.0 : nombreuses mises à jour !
  - MS07-057
    - Version 1.1 : mise à jour de la liste des fichiers affectés
  - MS07-058 DoS RPC
    - Version 1.1 : Windows XP x64 SP2 est aussi affecté
  - MS07-060 Faille Word
    - Version 1.1 : correction du lien Office 2004
    - Version 1.2 : problèmes de stabilité documentés
  - MS07-067
    - Version 1.1 : précision sur le fait que ce bulletin remplace MS07-065

Dernières vulnérabilités
Infos Microsoft (1/4) - sorties

- Sorties logicielles
  - DreamScene en version finale pour Vista Ultimate
  - De nouveaux packs de langue pour Vista Ultimate
  - OneCare 2.0
  - "Viridian" CTP (l'hyperviseur Windows 2008)
    - http://www.microsoft.com/windowsserver2008/virtualization/install.mspx
    - http://blogs.technet.com/longhorn/archive/2007/10/05/nouvelles-e-demos-1er-pas-avec-windows-server-2008-installation-et-utilisation-de-windows-server-virtualization-ctp.aspx
  - Virtual Server 2005 R2 SP1
  - VMRC+
  - Microsoft Deployment RC1
    - Anciennement BDD 2007
  - Windows 2008 RC0
    - http://www.innovateonwindowsserver.com/

Dernières vulnérabilités
Infos Microsoft (2/4) - sorties

- Aperçu de Windows 7.0
  - http://www.istartedsomething.com/20071019/eric-talk-demo-windows-7-minwin/
  - La version Core, appelée "WinMin", devrait tourner avec 25 Mo de disque … et une interface en ASCII Art (!)

- Windows XP SP3 en beta test
  - Apporte des fonctions de Vista, comme NAP
  - "Pèse" 350 Mo …
  - Prévu pour Q2 2008
  - Références :
    - http://www.generation-nt.com/windows-xp-sp3-actualite-46188.html
    - http://4sysops.com/archives/windows-xp-sp3-news/

Dernières vulnérabilités
Infos Microsoft (3/4) - sécurité

- MSDN Magazine du mois de novembre
  - Spécial sécurité
    - http://msdn.microsoft.com/msdnmag/issues/07/11/Default.aspx?loc=fr
- Aperçu de quelques outils de sécurité internes à Microsoft
  - http://securitybuddha.com/2007/10/25/a-sneak-peak-at-some-cool-software-security-tools/
  - "XSS Detect" est disponible publiquement
    - http://blogs.msdn.com/ace_team/archive/2007/10/22/xssdetect-public-beta-now-available.aspx
- Attention à System.URI.AbsolutePath()
  - Ne protège pas aussi efficacement qu'on pourrait le pense
    - http://blogs.msdn.com/ace_team/archive/2007/10/10/system-uri-absolutepath-vs-phishing-attack.aspx

Dernières vulnérabilités
Infos Microsoft (4/4) - Vista

- Une commande à connaître : PERFMON /REPORT
  - http://blogs.technet.com/longhorn/archive/2007/10/05/le-rapport-cach-du-moniteur-de-performances-vista.aspx
- ReadyBoost, inutile ?
  - http://4sysops.com/archives/vista-readyboost-doesn%e2%80%99t-improve-performance/
- Linux Vixta (!)
  - http://vixta.sourceforge.net/index.php
- Le Month of Vista Bugs, c'est parti
  - http://movb.blogspot.com/

Dernières vulnérabilités
Autres avis (1/10) – failles

- La "faille PDF" n'en finit pas
  - Détails techniques :
    - Le problème est lié au fonctionnement de ShellExecute() lorsque IE 7 est installé
    - De nombreuses applications tierces ne filtrent pas correctement les URI
    - http://www.heise-security.co.uk/news/96982
    - http://research.eeye.com/html/alerts/zeroday/20070725.html
  - Preuve de concept :
    - http://www.nthelp.com/test.pdf
  - Workaround pour Adobe :
    - http://www.adobe.com/support/security/advisories/apsa07-04.html
    - Finalement corrigé par Acrobat 8.1.1
  - La presse en parle :
    - http://www.reuters.com/article/internetNews/idUSN10234831200710 10

Dernières vulnérabilités
Autres avis (2/10) – failles

- Firefox 2.0.0.8
  - Corrige plusieurs problèmes de sécurité, dont le précédent
- Firefox 2.0.0.9
  - Corrige plusieurs failles dont :
    - http://www.gnucitizen.org/blog/bugs-in-the-browser-firefoxs-data-url-scheme-vulnerability
- QuickTime 7.3
  - Corrige plusieurs failles de sécurité
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=620
    - CVE-2007-2395, CVE-2007-3750, CVE-2007-3751, CVE-2007-4672, CVE-2007-4675, CVE-2007-4677
- AOL ActiveX Radio (AmpX)
  - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=623
- SysInternals DbgView
  - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=621
  - Pas idiot car le driver 64 bits est signé

Dernières vulnérabilités
Autres avis (3/10) – failles

- Un "0day" dans le composant ActiveX de RealPlayer exploité dans la nature
  - Affecte : ierpplug.dll
  - Détails :
    - http://www.avertlabs.com/research/blog/index.php/2007/10/19/realplayer-zero-day-exploit-hits-the-web/
    - http://research.eeye.com/html/alerts/zeroday/20071019.html
  - Un correctif a été publié en 24h
  - Conséquence : la NASA demande à tous ses employés de ne plus utiliser IE !
    - http://www.infosecblog.org/2007/10/nasa-bans-ie.html

Dernières vulnérabilités
Autres avis (4/10) – failles

- Faille dans le pilote MacroVision "secdrv.sys"
  - Utilisé par la protection "SafeDisc" (entre autres)
  - Permet l'exécution de code en Ring0
  - Détails :
    - http://research.eeye.com/html/alerts/zeroday/20071016.html
  - Mise à jour :
    - http://www.macrovision.com/promolanding/7352.htm
  - Note : la faille a été "redécouverte" en 24h après la publication d'un message sur le blog de Symantec
    - http://www.symantec.com/enterprise/security_response/weblog/2007/10/privilege_escalation_exploit_i.html
    - http://www.reversemode.com/index.php?option=com_content&task=view&id=43&Itemid=1

Dernières vulnérabilités
Autres avis (5/10) – failles

- Java 1.6.0 update 3 : c'était une mise à jour de sécurité …
  - Elévation de privilège
    - http://sunsolve.sun.com/search/document.do?assetkey=1-26-103112-1
  - Problème d'isolation inter-domaines sur un message HTTP 302
  - La liste complète (?) :
    - DNS Rebinding
      - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5232
    - Fuite d'informations sur l'emplacement du cache local
      - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5238
    - Evasion de la sandbox lors d'un drag-n-drop
      - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5239
    - Masquage d'une fenêtre d'alerte
      - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5240
    - Evasion de l'isolation inter-domaines via DNS Multi-pinning
      - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5273
    - Idem via LiveConnect
      - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5274

Dernières vulnérabilités
Autres avis (6/10) – malware et spam

- Le spam MP3
  - http://www.avertlabs.com/research/blog/index.php/2007/10/18/youve-got-mp3-mail/
- Un virus Mac OS X réellement trouvé "dans la nature"
  - Arrive sous forme de pseudo-codec au format ".DMG"
  - Reconfigure le serveur DNS
  - Les premières versions ne ciblent que "adultfriendfinder.com"
  - Références :
    - http://www.intego.com/news/ism0705.asp
    - http://www.avertlabs.com/research/blog/index.php/2007/10/31/puper-zlob-what-are-the-attackers-targeting/
- Un autre moyen de lutter contre le spam : l'intimidation
  - http://www.avertlabs.com/research/blog/index.php/2007/10/11/two-dead-spammers/

Dernières vulnérabilités
Autres avis (7/10) – malware et spam

- Analyse du "Storm Worm"
  - http://www.cyber-ta.org/pubs/StormWorm/
- Rapport du PhishTank
  - http://media.washingtonpost.com/wp-srv/technology/documents/PhishTank_Annual_Report_10-9-07.pdf
  - Le premier hébergeur de phishing français, Free, se classe 7ème ☺
- DrWeb propose le scan de liens "en ligne" intégré au navigateur
  - Plugins :
    - http://www.freedrweb.com/browser/mozilla+firefox/
    - http://www.freedrweb.com/browser/internet+explorer/
    - http://www.freedrweb.com/browser/opera/
- ZoneAlarm se met au "sandboxing" de navigateur
  - http://www.svmlemag.fr/actu/01838/zone_alarm_force_field_un_champ_de_force_autour_du_navigateur

Dernières vulnérabilités
Autres avis (8/10) – malware et spam

- Utiliser des humains pour contourner des captchas
  - http://vil.nai.com/vil/content/v_143504.htm
- Les génies du marketing frappent encore
  - http://www.unitedviruses.org/index.htm

Dernières vulnérabilités
Autres avis (9/10) – attaques 2.0

- ECMAScript 4 va-t-il dans la bonne direction ?
  - http://www.riffraff.info/2007/10/25/ecmascript-4-the-fourth-system-syndrome
- "Pénétrer le réseau des opérateurs est tellement facile, même un homme des cavernes aurait pu y arriver"
  - Source : Robert Moore
    - http://www.informationweek.com/news/showArticle.jhtml?articleID=202101781
    - http://taosecurity.blogspot.com/2007/09/be-caveman.html
- Une maison prise d'assaut après un piratage du "911"
  - L'auteur du piratage a 18 ans
  - http://www.pcworld.com/article/id,138591-c,hackers/article.html
- Le 11 novembre 2007 réservé pour le cyber-jihad
  - Pas vraiment au point
    - http://www.theregister.co.uk/2007/11/02/cyber_jihad_rumours/
    - http://www.avertlabs.com/research/blog/index.php/2007/11/09/cyber-jihad-isnt-here-yet/

Dernières vulnérabilités
Autres avis (10/10) – attaques 2.0

- Une "démo" de cyberattaque par le DHS
  - http://youtube.com/watch?v=fJyWngDco3g
- 100 ambassades piratées
  - http://www.derangedsecurity.com/deranged-gives-you-100-passwords-to-governments-embassies/
  - Simplement en "sniffant" sur un nœud de sortie Tor
- Encore une affaire de fuite d'information
  - http://www.cnn.com/2007/SHOWBIZ/10/10/clooney.records/index.html
- Une faille comme on en voit plus …
  - Affecte : LiteSpeed Web Server 3.2.3
  - Exploit : %00.txt à la fin de l'URL permet d'avoir accès au source PHP
- Le Web 2.0 sans l'effet bisounours
  - http://www.hatebook.org/

Dernières vulnérabilités
Autres infos (1/3) – just for fun

- SafeBoot racheté $350m par McAfee
  - http://www.vulnerabilite.com/mcaffe-safeboot-protection-donnee-rachat-actualite-20071010010950.html
  - Encore une société européenne qui s'en va …
- Trend Micro rachète Provilla
  - http://www.lesnouvelles.net/articles/business/906-trend-micro-achete-provilla.html
  - Spécialiste de la lutte contre la fuite d'information
- Le fondateur de WabiSabiLabi (Roberto Preatoni) arrêté
  - (Accessoirement fondateur de Zone-H)
  - Voir :
    - http://www.matasano.com/log/992/wabisabilabi-co-founder-arrested/
    - http://wabisabilabi.blogspot.com/
    - http://en.wikipedia.org/wiki/Roberto_Preatoni

Dernières vulnérabilités
Autres infos (2/3) – just for fun

- La Saga iPhone continue
  - Faille dans LibTIFF (firmware 1.1.1)
  - Complètement exploité par Metasploit
    - http://toc2rta.com/?q=node/30
    - http://blog.metasploit.com/
  - Un patch "non officiel" est disponible (!)
    - http://www.cse.msu.edu/~dunham/touch/
    - Il peut être installé via Metasploit (!!)
  - La politique Apple : "Hack Us? No, Hack You!"

- La Nuit Blanche, c'est sur Second Life aussi
  - http://www.01net.com/editorial/360809/second-night-une-nuit-blanche-sur-second-life/

Dernières vulnérabilités
Autres infos (3/3)

- Et pendant ce temps là sur la mailing liste de l'OSSIR
  - Liste SUR
    - Sun Java System Identity Manager
    - Faille Acrobat 8.1 et diversité logicielle
    - Tracking des internautes par JavaScript
    - Proxy CVS / SVN / HG
    - IPFilter et connexions SSH
    - Divulagtion de vulnérabilités
    - Centralisation des logs et corrélation
  - Liste NT
    - Retrouver des messages effacés dans Outlook
    - Conférence de Thierry Zoller à Hack.lu sur l'attaque des antivirus
      - Voir aussi : http://blog.didierstevens.com/2007/10/23/a000n0000-0000o000l00d00-0i000e000-00t0r0000i0000c000k/

Questions / réponses

- Questions / réponses
- Date de la prochaine réunion
  - Prochaine réunion le 10 décembre 2007
- N'hésitez pas à proposer des sujets et des salles