OSSIR
Groupe Sécurité Windows

Réunion du 7 juillet 2008

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

Jérémy LEBOURDAIS
jeremy.lebourdais (à) edelweb.fr

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

Dernières vulnérabilités
Avis Microsoft

- **Correctifs de Juin 2008**

  - **MS08-030 Vulnérabilité BlueTooth**
    - **Affecte : Windows XP SP2/SP3, Vista SP0/SP1**
    - **Exploit : requêtes SDP multiples**
      - **Difficile à exploiter**
        - **http://blogs.technet.com/swi/archive/2008/06/10/ms08-030-all-bark-and-no-bite-the-case-of-the-bluetooth-update.aspx**
    - **Crédit : n/d**

  - **MS08-031 Patch cumulatif pour IE**
    - **Affecte : IE toutes versions supportées**
    - **Exploit :**
      - **Exécution de code via une corruption mémoire**
      - **"Request Header Cross-Domain Information Disclosure"**
    - **Crédit :**
      - **Sebastian Apelt, Peter Vreugdenhil, anonymous/ZDI**

Dernières vulnérabilités
Avis Microsoft

- MS08-032 Contrôle vocal du PC (!)
  - Affecte : Windows toutes versions supportées
  - Exploit :
    - Speech API (sapi.dll) : dicter des commandes via un fond sonore dans une page Web ...
    - Bloque également l'ActiveX "BackWeb" (souvent inclus avec Logitech)
  - Crédit : n/d

- MS08-033 Failles multiples dans DirectX
  - Affecte : DirectX toutes versions supportées
  - Exploit : flux MJPEG et SAMI
    - http://blogs.technet.com/swi/archive/2008/06/10/ms08-033-so-what-breaks-when-you-acl-quartz-dll.aspx
  - Crédit :
    - Mark Dowd / ISS X-Force
    - anonymous/ZDI

Dernières vulnérabilités
Avis Microsoft

- MS08-034 Elévation de privilèges via WINS
  - Affecte : Windows 2000 SP4, Windows 2003 SP1/SP2
  - Exploit : envoi d'un paquet réseau malformé
    - Sur une socket locale
    - http://expertmiami.blogspot.com/2008/06/francaises-francais-time-to-bend-over.html
  - Crédit : n/d

- MS08-035 Déni de service LDAP
  - Affecte : AD LDS, ADAM et Active Directory, toutes versions supportées
  - Exploit : déni de service via une requête LDAP malformée
  - Crédit : Alex Matthews + John Guzik / Securify

Dernières vulnérabilités
Avis Microsoft

- MS08-036 Déni de service via PGM
  - Affecte : Windows toutes versions supportées (sauf Windows 2000)
  - Exploit : 2 failles dans le traitement des requêtes PGM
    - PGM = Pragmatic General Multicast – RFC 3208
    - http://blogs.technet.com/swi/archive/2008/06/10/ms08-036-pgm-what-is-pgm.aspx
  - Crédit : n/d
  - Remarque : PGM est installé avec MSMQ

- Autres mises à jour
  - Mises à jour firmwares/signatures/etc.
    - http://technet.microsoft.com/en-us/wsus/bb466214.aspx
  - Mise à jour de la page WSUS
    - http://support.microsoft.com/kb/894199

Dernières vulnérabilités
Avis Microsoft

- **Prévisions pour Juillet 2008**
  - **Bulletin #1**
    - **Affecte : SQL Server 7 / 2000 / 2005**
    - **Exploit : élévation de privilèges**
  - **Bulletin #2**
    - **Affecte : Windows Vista / 2008**
    - **Exploit : exécution de code à distance**
  - **Bulletin #3**
    - **Affecte : Windows 2000 / XP / 2003 / 2008**
    - **Exploit : "spoofing" (?)**
  - **Bulletin #4**
    - **Affecte : Exchange 2003 / 2007**
    - **Exploit : élévation de privilèges**
  - **+ mise à jour du client Windows Update**

Dernières vulnérabilités
Avis Microsoft

- Advisories
  - Q954474
    - serveur System Center Configuration Manager 2007
    - + client SMS 2003 clients
    - = pas de mises à jour en juin
  - Q954960
    - WSUS 3.0 + Office 2003 = pas de mises à jour
  - Q954462
    - Prévalence des attaques par injection SQL sur Internet : des contremesures
      - UrlScan version 3.0 Beta
      - Microsoft Source Code Analyzer for SQL Injection Community Technology Preview (June 2008)
      - Scrawlr Scanner (HP + Microsoft)

Dernières vulnérabilités
Avis Microsoft

- **Révisions**
  - **MS06-078**
    - **Version 5.0 : Windows XP SP3 est affecté**
    - **Version 6.0 : Media Player 6.4 / Windows XP SP3 n'est pas affecté**
  - **MS07-042 (faille XML)**
    - **Version 4.0 : Windows XP SP3, Vista SP1 et Windows 2008 sont affectés**
  - **MS07-068**
    - **Version 2.0 : Windows XP SP3 est affecté**
    - **Version 2.1 : mise à jour de la FAQ**
  - **MS08-030**
    - **Version 2.0 : nouvelle version du patch**

Dernières vulnérabilités
Infos Microsoft - sorties

- Sorties logicielles
  - IE 8 Beta 1 sur Windows Update
  - IE 8 Beta 2 prévu pour août
    - Pourra être "slipstreamé"
    - Anti-phishing amélioré (SmartScreen)
    - Anti-XSS
    - Et beaucoup d'autres ...
      - http://blogs.msdn.com/ie/archive/2008/07/02/ie8-security-part-v-comprehensive-protection.aspx
  - Hyper-V RTM
  - SilverLight 2 Beta 2
  - SQL Server 2008 RC0

Dernières vulnérabilités
Infos Microsoft

- Microsoft privé d'appels d'offre européens ?
  - http://www.lemondeinformatique.fr/actualites/lire-bruxelles-livre-un-blanc-seing-aux-27-pour-ecarter-microsoft-des-appels-d-offre-26360.html
- La normalisation d'Office Open XML suspendue
  - http://www.lemondeinformatique.fr/actualites/lire-la-standardisation-d-ooxml-suspendue-par-un-appel-26302.html
- Microsoft ajoute "Taterf" et "Frethog" au MSRT
  - Malwares ciblant des jeux en ligne
  - Presque 1 million de détections en 1 semaine
    - http://fasthorizon.blogspot.com/2008/06/microsoft-wipes-out-700000-too-late-to.html
- Stallman vs. Gates (again)
  - http://news.bbc.co.uk/2/hi/technology/7487060.stm

Dernières vulnérabilités
Infos Microsoft

- Hyper-V vs. RHEL 5 (Xen)
  - http://www.microsoft.com/windowsserver/compare/ReportsDetails.mspx?recid=69
  - http://www.microsoft.com/windowsserver/compare/webcasts/Windows-server-2008-HyperV-vs-Linux-Hypervisor.mspx
- Windows Seven et multi-touch
  - http://blogs.msdn.com/frogzfr/archive/2008/05/29/premieres-demonstrations-de-windows-seven.aspx
- Technet Magazine, Juin 2008
  - Au sommaire : la sécurité par l'obscurité
  - http://technet.microsoft.com/fr-fr/magazine/cc510382(TechNet.10).aspx
- La communication Microsoft, encore et toujours ☺
  - http://www.server-quest.com/

Dernières vulnérabilités
Infos Microsoft - Vista

- **Une conférence à suivre ...**
  - **http://www.blackhat.com/html/bh-usa-08/bh-usa-08-speakers.html#Sotirov**

- **Intel ne passera pas à Vista**
  - **http://www.lemondeinformatique.fr/actualites/lire-intel-a-decide-de-ne-pas-s-equiper-en-vista-26445.html**

Dernières vulnérabilités
Autres avis – failles

- Produits tiers vulnérables
  - QuickTime < 7.5
  - VLC < 0.8.6h
  - Safari < 3.1.2
    - http://support.apple.com/kb/HT2092
  - Acrobat Reader 8.1.2
    - http://www.adobe.com/support/security/bulletins/apsb08-15.html
  - FireFox < 2.0.0.15
  - Opera < 9.0.51

  - FireFox 3.0 bat le record du logiciel le plus téléchargé en 24h
    - Sortie officielle le 17 juin
    - Et de la faille la plus rapide ?
      - http://dvlabs.tippingpoint.com/blog/2008/06/18/vulnerability-in-mozilla-firefox-30

  - FreeType2 (affecte Sun JRE)
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=715
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=716
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=717

Dernières vulnérabilités
Autres avis – failles

- Internet Explorer 6
  - Affecte : IE 6 uniquement
  - Exploit : "cross domain scripting"
    - Les propriétés "location" et "location.href" ne sont pas correctement vérifiées
    - http://raffon.net/research/ms/ie/crossdomain/string.html

Dernières vulnérabilités
Autres avis – malwares et spam

- BlogSpot : 75% de "splogs"
  - http://www.infoniac.com/hi-tech/google-blogs-spam.html
- Lutter contre le phishing de manière éducative
  - AT&T remplace un faux numéro d'appel par un message éducatif
    - http://www.avertlabs.com/research/blog/index.php/2008/06/20/vishing-takedown-best-practice/
- Le Messaging Anti-Abuse Working Group (MAAWG) publie ses "best practices"
    - http://www.maawg.org/news/maawg080625

Dernières vulnérabilités
Autres avis – attaques 2.0

- Amazon *down*, aucune explication
  - http://isc.sans.org/diary.html?storyid=4532
- 637 millions de browsers pas à jour
  - http://blogs.iss.net/archive/TheWebBrowserThreat.html
  - Source : Google
- L'Espagne n'a pas tout gagné
  - http://asert.arbornetworks.com/2008/06/spain-wins-euro-2008-comes-under-ddos-attack/
- 378,000 machines infectées en 16 mois
  - Via un PsExec backdooré
  - http://securite.reseaux-telecoms.net/actualites/lire-un-peu-de-patience-mene-a-une-veritable-infection-18452.html

Dernières vulnérabilités
Autres avis – actualités

- Yahoo! n'a pas perdu de temps
  - http://www.lejdd.fr/cmc/economie/200824/pub-yahoo-signe-avec-google_125282.html
- Une grosse affaire d'espionnage interne chez Deutsche Telekom
  - http://www.01net.com/editorial/381451/comment-empecher-la-fuite-de-donnees-sensibles-./
- Le "livre blanc de la Défense"
  - Où il est question de lutte informatique offensive ...
    - http://www.lemondeinformatique.fr/actualites/lire-la-lutte-contre-la-guerre-informatique-declaree-priorite-du-gouvernement-26358.html
- Capture du code PIN sur des ATM Citibank
  - http://www.heise-online.co.uk/security/Citibank-ATM-network-hacked--/news/111045

Dernières vulnérabilités
Autres avis – actualités

- Peut-on avoir confiance dans "la charte de la confiance en ligne" ?
  - http://www.pcinpact.com/actu/news/44018-filtrage-internet-neutralite-FAI-operateurs.htm
  - 1 an de préparation
    - http://www.lepoint.fr/actualites-medias/exclusif-loi-antipiratage-un-an-de-tractations-secretes/1253/0/254615
- Mêmes principes dans le "paquet télécom" au niveau européen
  - http://www.zataz.com/communique-presse/17370/Internet-Libre_-bientot-la-fin.html

Dernières vulnérabilités
Autres avis – actualités

- Le rapport 2008 du CLUSIF
  - "Menaces Informatiques et Pratiques de Sécurité en France"
  - http://www.clusif.asso.fr/fr/production/sinistralite/docs/CLUSIF-rapport-2008.pdf
- Un nouveau consortium de vendeurs
  - ICASI : Industry Consortium for Advancement of Security on the Internet
  - http://www.icasi.org/
- 30 juin 2008 : le "D Day" pour IPv6
  - Toute l'administration américaine doit être compatible
- L'ouverture des TLD, une bonne idée ?
  - http://www.lesechos.fr/journal20080623/lec1_une/4744299.htm
  - http://securitylabs.websense.com/content/Blogs/3118.aspx

Dernières vulnérabilités
Autres avis – just for fun

- Ne pas débloquer son iPhone trop vite ☺
  - http://www.maclife.com/article/teens_busted_for_hacking_iphone_in_apple_store
- La faille était dans la machine à café
  - http://news.cnet.com/8301-10784_3-9970757-7.html?tag=cnetfd.blogs.item
- Ou dans le mug !
  - http://www.infsec.cs.uni-sb.de/~unruh/publications/reflections.pdf
- Un voleur identifié ... par une carte SD WiFi
  - http://www.bestofmicro.com/actualite/25097-eye-fi.html

Dernières vulnérabilités
Autres avis – just for fun

Questions / réponses

- Questions / réponses
- Attention !
  - Il n'y aura plus qu'un seul groupe parisien à la rentrée
  - Prochaine réunion le mardi 9 septembre 2008
- N'hésitez pas à proposer des sujets et des salles
- Et bonnes vacances !