OSSIR
Groupe Sécurité Windows

Réunion du 10 septembre 2007

Revue des dernières vulnérabilités Microsoft

Cette veille est réalisée par les coanimateurs du groupe Windows

EdelWeb

Olivier REVENU
EdelWeb
olivier.revenu (à) edelweb.fr

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

Dernières vulnérabilités
Avis Microsoft (1/10)

- **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
  - Les systèmes affectés sauf mention contraire correspondent aux versions (Service Pack) actuellement supportées par l'éditeur

Dernières vulnérabilités
Avis Microsoft (2/10)

- **Correctifs de Juillet 2007**

  - **MS07-036 Failles multiples dans Excel**
    - **Affecte : Excel toutes versions supportées (2000 -> 2007)**
    - **Exploit : exécution de code**
      - **CVE-2007-1756, CVE-2007-3029, CVE-2007-3030**
    - **Crédit : n/d**

  - **MS07-037 Faille dans Publisher**
    - **Affecte : Publisher 2007**
    - **Exploit : exécution de code**
      - **CVE-2007-1754**
    - **Crédit : eEye**

Dernières vulnérabilités
Avis Microsoft (3/10)

- MS07-038 Faille dans le firewall Vista
  - Affecte : Vista toutes versions supportées
  - Exploit : fuite d'information
    - Il est possible de scanner une machine via Teredo
  - Crédit : Jim Hoagland & Ollie Whitehouse / Symantec

- MS07-039 Failles multiples dans Active Directory
  - Affecte : Windows toutes versions "serveur" supportées
  - Exploit :
    - Exécution de code à distance via une requête LDAP malformée
    - Déni de service (Windows 2000 uniquement)
  - Crédit :
    - Peter Winter-Smith / NGSSoftware
    - Neel Mehta / IBM Internet Security Systems X-Force

Dernières vulnérabilités
Avis Microsoft (4/10)

- **MS07-040 Failles multiples dans .NET Framework**
  - **Affecte : .NET Framework toutes versions supportées**
  - **Exploit :**
    - **Problème dans le loader PE (contournement de la sandbox)**
    - **Problème dans le compilation JIT (contournement de la sandbox)**
    - **Récupération du code source des pages ASP via une chaine *NULL-terminated***
  - **Crédit :**
    - **Dinis Cruz / OWASP**
    - **Paul Craig / Security Assessment**
    - **Jeroen Frijters / Sumatra**
    - **Ferruh T. Mavituna / Portcullis Computer Security Ltd.**

- **MS07-041 Faille dans IIS**
  - **Affecte : IIS 5.1 (Windows XP SP2)**
  - **Exploit : exécution de code à distance**
    - **Faille connue depuis 2005 (CVE-2005-4360) mais qui s'avère exploitable**
    - **http://www.securityfocus.com/archive/1/archive/1/419707/100/0/threaded**
  - **Crédit :**
    - **Jonathan Afek & Adi Sharabani / Watchfire**

Dernières vulnérabilités
Avis Microsoft (5/10)

- **Correctifs de Août 2007**
  - **MS07-042 Patch cumulatif pour MSXML**
    - **Affecte : MS-XML (toutes versions supportées, y compris Vista)**
    - **Exploit : déni de service et exécution de code**
    - **Crédit : iDefense, ZDI**
  - **MS07-043 Faille OLE**
    - **Affecte : Windows toutes versions supportées sauf Vista + Office 2004 + Visual Basic 6 SP6**
    - **Exploit : exécution de code**
    - **Crédit : iDefense, ZDI**
  - **MS07-044 Faille Excel**
    - **Affecte : Excel 2000, XP, 2003, 2004 + Excel Viewer 2003**
    - **Exploit : exécution de code**
    - **Crédit : Dyon Balding / Secunia Research**

Dernières vulnérabilités
Avis Microsoft (6/10)

- **MS07-045 Patch cumulatif pour IE**
  - **Affecte : IE toutes versions supportées**
  - **Exploit : 3 nouvelles failles corrigées**
  - **Crédit :**
    - **Hu Qianwei / NSFOCUS Security Team**
    - **Brett Moore / Security-Assessment.com**

- **MS07-046 Patch cumulatif pour la faille WMF**
  - **Affecte : W2000 SP4, XP SP2, XP x64, 2003 SP1, 2003 x64, 2003 SP1 Itanium**
  - **Exploit : nouvelle faille WMF**
  - **Crédit : eEye Digital Security**

- **MS07-047 Exécution de code via les "skins"**
  - **Affecte : Windows Media Player toutes versions supportées (7, 9, 10, 11)**
  - **Exploit : décompression des fichiers de skin et parsing de l'entête d'informations du fichier skin**
  - **Crédit : Piotr Bania, Dan Kaminsky**

Dernières vulnérabilités
Avis Microsoft (7/10)

- **MS07-048 Faille dans les gadgets Vista**
  - **Affecte : Vista 32 et 64 bits**
  - **Exploit : exécution de code à travers les flux RSS**
  - **Crédit : Aviv Raff / Fijan, iDefense**

- **MS07-049 Evasion de machine virtuelle**
  - **Affecte : Virtual PC sauf 2007, Virtual Server sauf 2005 R2 SP1**
  - **Exploit : évasion de la machine virtuelle**
    - **Requière d'être administrateur sur le *guest***
  - **Crédit : Rafal Wojtczuk / McAfee Avert Labs**

- **MS07-050 Patch cumulatif pour la faille VML**
  - **Affecte : IE toutes versions supportées**
  - **Exploit : nouvelle faille VML**
  - **Crédit :Derek Soeder / eEye Digital Security**

Dernières vulnérabilités
Avis Microsoft (8/10)

- **Prévisions pour Septembre 2007**

  - **1 bulletin critique affectant**
    - **Windows 2000 SP4**
  - **3 bulletins importants affectant**
    - **Visual Studio (toutes versions supportées)**
    - **SFU (toutes versions supportées) et sous-système POSIX**
    - **MSN Messenger (toutes versions supportées)**

  - **Un patch "important" pour SharePoint 3.0 a "disparu"**

Dernières vulnérabilités
Avis Microsoft (9/10)

- Advisories
  - Q932596 : mise à jour de Kernel Patch Protection (PatchGuard)
    - http://www.microsoft.com/technet/security/advisory/932596.mspx

- Révisions
  - MS07-036
    - Version 2.0 : sont également affectés Office 2004 pour Mac, Office 2007 Compatibility Pack
  - MS07-038
    - Version 1.1 : CVE incorrect
  - MS07-039
    - Version 1.1 : précision sur ADAM
  - MS07-040
    - Version 1.1 :
      - Rating "important" sur Vista
      - Version "mscordacwks.dll" incorrecte
      - Les utilisateurs de .NET 3.0 doivent néanmoins installer le patch 2.0
      - FAQ pour les développeurs ASP.NET
    - Version 1.2 : ???
    - Version 1.3 : les mises à jour sont cumulatives et peuvent inclure des corrections "non sécurité"

Dernières vulnérabilités
Avis Microsoft (10/10)

- MS07-041
  - Version 1.1 : précision sur le composant affecté (module de statistique)
- MS07-042
  - Version 1.1 : correction du "manifest" pour XML Core Services 4
- MS07-044
  - Version 1.1 : mise à jour du lien de téléchargement
- MS07-045
  - Version 1.1 : correction de la clé de base de registre pour IE 7
  - Version 1.2 : limite sur les cookies passée de 20 à 50
- MS07-046
  - Version 1.1 : workarounds disponibles
- MS07-047
  - Version 1.1 : correction de la clé de base de registre
- MS07-050
  - Version 1.1 : correction des noms de fichiers pour IE 7 sur Windows 2003
  - Version 1.2 : correction de la clé de base de registre pour IE 7

Dernières vulnérabilités
Infos Microsoft (1/5) - sécurité

- Microsoft Malware Protection Center
  - http://www.microsoft.com/security/portal/
- Malware Removal Starter Kit
  - http://www.microsoft.com/technet/security/guidance/disasterrecovery/malware/default.mspx
- Catalogue de Windows Update
  - http://catalog.update.microsoft.com/
- Des hackers chez Microsoft
  - http://blogs.msdn.com/hackers/
- WGA non disponible le 25 août dernier
  - http://blogs.msdn.com/wga/archive/2007/08/25/validation-issue-fix.aspx
- Evaluation CC de Vista et Windows Server 2008
  - http://blogs.msdn.com/laurelle/archive/2007/08/21/windows-vista-et-windows-server-2008-en-route-pour-les-common-criteria.aspx
- Des machines virtuelles préconfigurées pour le poste de travail standard de l'administration américaine
  - http://www.cio.gov/documents/FDCC_memo.pdf

Dernières vulnérabilités
Infos Microsoft (2/5) - sorties

- Sorties logicielles
  - Network Monitor 3.1
  - Vista SP1 Beta1 (juillet 2007)
    - Version finale prévue pour novembre 2007
    - Accélération suite au procès Google vs. Windows Search ?
  - Windows Vista Service Life-Cycle Management
  - OneCare 2.0
  - Visual Studio 2008 Beta2 + .NET Framework 3.5 Beta2
  - Windows Home Server RC1
  - IronRuby Alpha
  - Active Directory Explorer 1.0 (SysInternals)
  - OCS 2007
  - Performance Point Server 2007
    - Lancement médiatique à NY le 20 septembre 2007
  - PowerShell facile avec PowerGUI
    - http://www.powergui.org/index
- Fin de support
  - SUS 1.0 : 10 juillet 2007

Dernières vulnérabilités
Infos Microsoft (3/5) – sorties prévues

- En 2008 …
  - Windows Vista SP1
    - http://www.guwiv.com/portal/blogs/news/archive/2007/08/29/vista-sp1-infos-exclusives.aspx
      - Corrige des bogues
      - Mais ajoute des fonctions de Windows Server 2008 également !
    - Windows Vista Service Pack 1 Beta White Paper
      - http://windowsvistablog.com/blogs/windowsvista/pages/windows-vista-service-pack-1-beta-whitepaper.aspx
  - Windows Server 2008 (27 février 2008)
    - Un site très "Web 2.0"
      - https://www.microsoft.com/servers/faces/default.aspx
  - SQL Server 2008
  - Visual Studio 2008
- En 2010
  - La prochaine version de Windows (version cliente)

Dernières vulnérabilités
Infos Microsoft (4/5) - actualité

- Microsoft Open Source (!)
  - http://www.microsoft.com/opensource
- La comparaison de Windows et de Linux selon Microsoft
  - http://www.microsoft.com/windowsserver/compare/default.mspx
- Outlook Voice Access : écoutez vos mails par téléphone
  - http://www.microsoft.com/exchange/evaluation/unifiedmessaging/umcommunications.mspx
- Microsoft vous occupe pendant vos vacances
  - http://msdn2.microsoft.com/fr-fr/aboutmsdn/bb625975.aspx

Dernières vulnérabilités
Infos Microsoft (5/5) – docs

- Responding to IT Security Incidents
  - http://www.microsoft.com/technet/security/guidance/disasterrecovery/responding_sec_incidents.mspx/sce
- Guide de sécurité IE 7
  - http://www.microsoft.com/downloads/details.aspx?FamilyId=6AA4C1DA-6021-468E-A8CF-AF4AFE4C84B2&displaylang=en
- Group Policy Settings Reference pour Windows Server 2008 Beta3
  - http://www.microsoft.com/downloads/details.aspx?familyid=2043b94e-66cd-4b91-9e0f-68363245c495&displaylang=en
- Guides Step by Step pour Windows Serveur 2008
  - http://www.microsoft.com/downloads/details.aspx?FamilyID=518d870c-fa3e-4f6a-97f5-acaf31de6dce&DisplayLang=en#filelist
- Écrire des gadgets sécurisés sous Vista (Howard)
  - http://msdn2.microsoft.com/en-us/library/bb498012.aspx
- Integrity Mechanism Technical Reference
  - http://msdn2.microsoft.com/en-us/library/bb625964.aspx

Dernières vulnérabilités
Infos Vista (1/3)

- 60 millions de licences Vista vendues au 30 juin 2007
  - Source : Microsoft
- Des outils pour calculer le coût des licences Vista
  - LicenceWise
  - Microsoft Vista business Value Assessment
- 2 "gros" patches pre-SP1
  - Q938979 et Q938194
  - Tout simplement … indispensables !
- Vista compatible avec 95% des logiciels
  - http://support.microsoft.com/gp/VistaCompatibility/fr
- Vista + Son + Réseau = problème
  - http://it.slashdot.org/article.pl?sid=07/08/21/1441240
  - http://blogs.technet.com/markrussinovich/archive/2007/08/27/1833290.aspx

Dernières vulnérabilités
Infos Vista (2/3) – hors Microsoft

- Vista trop bavard ?
  - http://news.softpedia.com/news/Forget-about-the-WGA-20-Windows-Vista-Features-and-Services-Harvest-User-Data-for-Microsoft-58752.shtml
- La DRM Windows Media 11 crackée
  - http://www.generation-nt.com/microsoft-protection-drm-fairuse-windows-media-actualite-43219.html
- Microsoft Works gratuit ! Mais avec de la publicité …
  - http://www.generation-nt.com/microsoft-woks-publicite-gratuit-actualite-43785.html
- Vista pour $8 … en Iran !
  - http://digg.com/tech_news/Pirated_Version_of_Windows_Vista_Selling_for_8_in_Iran

Dernières vulnérabilités
Infos Vista (3/3) – hors Microsoft

- **Charger des drivers non signés sous Vista 64**
  - **Méthode #1 : un driver signé spécifique**
    - **Ex. ATSIV**
      - **http://www.linchpinlabs.com/resources/atsiv/usage-design.htm**
    - **Masque également le driver dans la liste des modules chargés**
      - **Une pure fonction de rootkit !**
    - **Déjà bloqué par Microsoft …**
      - **http://blogs.msdn.com/windowsvistasecurity/archive/2007/08/03/x64-driver-signing-update.aspx**
  - **Méthode #2 : une faille dans un driver existant**
    - **Ex. Purple Pill (Alex Ionescu + 90210)**
      - **http://it.slashdot.org/it/07/08/10/0448207.shtml**
    - **Beaucoup plus difficile à bloquer …**

Dernières vulnérabilités
Autres avis (1/10) – failles

- Exécution de commandes arbitraires dans IE
  - Affecte : IE lorsque FireFox est également installé
    - (et Safari pour Windows, accessoirement)
  - Exploit :
    - http:///larholm.com/2007/07/10/internet-explorer-0day-exploit/
    - http:///larholm.com/vuln/firefoxurl.html
  - Faille liée :
    - http:///labs.idefense.com/intelligence/vulnerabilities/display.php?id=565
  - Corrigé par FireFox 2.0.0.5 (et définitivement par FireFox 2.0.0.6)
    - Note : FireFox 1.5 n'est plus supporté

- Faille(s) Flash
  - Affecte : Flash < 9.0.47
  - Exploit : CVE-2007-3456, CVE-2007-3457, CVE-2007-2022

- Faille QuickTime
  - Affecte : QuickTime < 7.2
  - Exploit : integer overflow dans le traitement des fichiers SMIL
  - Remarque : QuickTime > 7.1.6 n'est pas supporté sous Windows 2000

Dernières vulnérabilités
Autres avis (2/10) – failles

- Elévation de privilège locale dans Winpcap
  - Affecte : Winpcap < 4.0.1
  - Exploit : faille dans l'interface du driver (=> exécution de code dans le noyau)

- Faille dans le traitement des images TGA par DirectX
  - Affecte : DirectX SDK antérieur au octobre 2006
  - Exploit : image Targa malformée
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=562

- Faille dans mDNS
  - Affecte : Mac OS X
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=573
    - http://docs.info.apple.com/article.html?artnum=306172
  - Même faille ?
    - http://infosecsellout.blogspot.com/2007/07/oh-look-apple-worm.html

- Note : il y a eu trop de failles dans les antivirus pour les mentionner ici …

Dernières vulnérabilités
Autres avis (3/10) – failles

- Java 6 Update 2
  - Failles dans le traitement des fichiers JPEG et BMP
    - http://www.auscert.org.au/render.html?it=7664
    - http://news.zdnet.com/2100-1009_22-6196493.html
  - Injections de commandes dans la signature XML
    - http://www.isecpartners.com/files/XMLDSIG_Command_Injection.pdf

- Un 0Day … d'il y a 7 ans !
  - Affecte : Office 2000
  - http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1256184,00.html

- Oracle Quaterly Patch
  - 45 failles corrigées

- Service "eEye Preview"
  - Des "0day" … jusqu'à 1 an avant leur correction
  - http://research.eeye.com/html/services/

Dernières vulnérabilités
Autres avis (4/10) – failles

- Faille Yahoo! Messenger (sur le support Webcam)
  - Affecte : Messenger 8.1 avant le 21 août 2007
  - http://messenger.yahoo.com/security.php
  - http://research.eeye.com/html/alerts/zeroday/20070812.html
  - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=591
- Faille MSN Messenger (Webcam également !)
  - Affecte : Messenger 6 et 7
  - http://secunia.com/advisories/26570/
- Trop d'obfuscation (JavaScript) nuit à la compatibilité
  - IE et FireFox n'interprètent pas de la même manière "arguments.callee.toString()"
  - Résultat : FireFox est protégé contre les codes les mieux protégés ☺
- Mozilla s'engage à corriger toute faille en moins de 10 jours
  - http://ha.ckers.org/blog/20070803/mozilla-says-ten-fucking-days/

Dernières vulnérabilités
Autres avis (5/10) – malwares et spam

- Après le spam PDF :
  - Le spam ZIP
  - Le spam Excel
  - Le spam numérique (6 chiffres + 8 caractères hexa)
  - Le spam FDF
  - Le spam "RegExp"
    - … [a][v][e] alread-y {s}e(e)[n] CYTV#'s m^arket i_mpact bef+ore …
- Très forte activité du gang "Zhelatin"
  - Créativité sans limite
    - Faux login/mdp, fausses vidéos, …
  - Objectif : recrutement pour un botnet
    - http://yom.retiaire.org/doku.php?id=zhelatin_ou_storm_worm_le_retour
- Contournement astucieux de WFP
  - Deux API non documentées permettent de désactiver le système !
    - http://www.avertlabs.com/research/blog/index.php/2007/07/05/wfp-hack-redefined/
- Du "bulletproof hosting" … en lien sponsorisé !
  - http://www.f-secure.com/weblog/archives/archive-072007.html#00001233

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

- Un virus qui infecte les pages HTML
  - Rajoute un lien vers une IFRAME malicieuse
  - http://vil.nai.com/vil/content/v_142982.htm
- Joe Job : le spam comme outil d'atteinte à la réputation
  - http://en.wikipedia.org/wiki/Joe_job
- Un rootkit dans le driver des clés Sony USB Microvault
  - http://www.f-secure.com/weblog/#00001263
- Le kit Shark 2 pour créer rapidement des chevaux de Troie
  - http://www.theregister.com/2007/08/15/shark_trojan_creation_kit/
  - http://shark-project.net/
- Une attaque MiTM sur l'authentification 2-facteurs de ABN AMRO
  - https://www.abnamro.nl/nl/overabnamro/en_internet_crime.html
- Trojan, poker et terrorisme
  - http://www.f-secure.com/weblog/archives/archive-082007.html#00001247
  - http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501153.html

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

- Outil "BotHunter"
  - Détecte les comportements anormaux en bordure
    - http://www.cyber-ta.org/BotHunter/
  - Quelques exemples d'analyses
    - http://www.cyber-ta.org/releases/malware-analysis/public/
- Outil "Red Curtain"
  - Recherche les exécutables "anormaux" sur un système
    - http://www.mandiant.com/mrc
- Nkem Owoh arrêté dans le cadre d'une vaste opération en Hollande
  - L'auteur de "I Go Chop Your Dollar" …
- Un auteur de virus pour mobiles arrêté en Espagne
  - http://news.brisbanetimes.com.au/spanish-police-arrest-creator-of-mobile-phone-virus/20075024-k35.html
- Orange bloque le port TCP/25 en sortie depuis le 14 juin
- Quelques quizz rigolos
  - Phishing : http://www.siteadvisor.com/quizzes/phishing_0707/
  - Spyware : http://www.siteadvisor.com/quizzes/spyware_0306.html

Dernières vulnérabilités
Autres avis (8/10) – attaques 2.0

- Une intrusion qui sort du lot …
  - http://www.spectrum.ieee.org/print/5280
- Toujours plus d'attaques ciblées
  - Allemagne (attribuée à des chinois) : http://www.f-secure.com/weblog/#00001262
  - Japon : http://www.avertlabs.com/research/blog/index.php/2007/08/17/targeted-zero-day-attack-against-free-tools-lhaz/
  - France : http://www.lexpress.fr/info/infojour/reuters.asp?id=52690&1506
- Du racket dans Second Life
  - http://www.computerworld.com.au/index.php/id;463036027
- Plusieurs comptes de recruteurs volés sur Monster.com
  - 1,6 million d'utilisateurs ont reçu du spam !
  - http://isc.sans.org/diary.php?storyid=3295
- L'affaire TJX continue
  - http://www.eweek.com/article2/0,1895,2156263,00.asp

Dernières vulnérabilités
Autres avis (9/10) – juste fun

- Le groupe des utilisateurs Windows Server
  - http://www.guwise.com/
- Dell envisage de mettre un hyperviseur dans ses BIOS
  - Il ne peut en rester qu'un …
    - http://arstechnica.com/news.ars/post/20070808-dell-virtualization-on-motherboards.html
- Sony intente un procès à la société qui lui a fourni le "rootkit"
  - http://www.hollywoodreporter.com/hr/content_display/business/news/e3i214c26acb62c59b679bbbc3594def806
- Un certification trop loin ?
  - Certified Reverse Code Engineering Professional
    - http://www.iitac.org/content/view/26/110/lang,en/
  - Certified Unethical Security Systems Expert
    - http://www.cusse.org/
- We are safe … for now
  - http://www.zdnet.fr/actualites/informatique/0,39040745,39372613,00.htm
  - http://www.journal-officiel.gouv.fr/jahia/Jahia/marches-publics/pid/120?id=detail&pageToDisplay=detail&file=200708020066B.HTM&idAnnonce=1186042275072494185&numAnnonce=66&datePub=20070802000000&nomPub=BOMP%20B&numBulletin=20070147&departement=75&tetierR4=Appel%20d%20offres

Dernières vulnérabilités
Autres avis (10/10) - juste fun

- Une compagnie pornographique poursuit Microsoft
  - Motif : le moteur de recherche MSN permet de trouver ses images …
    - http://techno.branchez-vous.com/actualite/2007/08/une_compagnie_porno_poursuit_m.html
- Un logiciel de contrôle parental à 84M$ craqué en 30 minutes
  - http://www.zdnet.com.au/news/security/soa/Teen-cracks-AU-84-million-porn-filter-in-30-minutes/0,130061744,339281500,00.htm
- Du neuf avec du vieux: Vista dans une super NES
  - http://www.akihabaranews.com/fr/news-14560-Nintendo+Super+Famicom+Vista+power.html
- La pizza par texto
  - http://www.dominos.co.uk/smsexplainednotregistered.aspx
- T'as pas captché ?
  - http://www.tonsai.de/blog-english/2007/craziest-captchas-on-the-web/

Dernières vulnérabilités Histoires (1/4)

- La saga Facebook
  - Facebook : LE nouveau site de social networking
    - http://en.wikipedia.org/wiki/Facebook
    - Principalement utilisé par les étudiants
    - 34 millions d'utilisateurs en juillet 2007
  - Le code source de Facebook est dans la nature
    - http://www.0x000000.com/?i=418
  - Facebook court après …
    - … mais il devient impossible "d'effacer" une information
  - Facebook : le vol d'identité facile
    - http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html

Dernières vulnérabilités
Histoires (2/4)

- La saga Skype
  - Problème sur le réseau Skype le 16 août
    - http://heartbeat.skype.com/2007/08/problems_with_skype_login.html
  - Des explications assez fumeuses
    - http://heartbeat.skype.com/2007/08/what_happened_on_august_16.html
    - http://blogs.securiteam.com/?p=983
    - http://sid.rstack.org/blog/index.php/212-quand-skype-passe-au-rouge
  - Néanmoins le Patch Tuesday a un impact
    - http://www.theregister.co.uk/2007/08/16/186k_microsoft_security_bandwidth/
  - Des problèmes de confidentialité avec Skype ?
    - http://yro.slashdot.org/yro/07/08/26/1312256.shtml

Dernières vulnérabilités
Histoires (3/4)

- La saga iPhone

  - Faille dans le navigateur démontrée à BlackHat
    - Affecte : libPCRE 6.2
    - http://www.securityfocus.com/brief/552
  - Un patch disponible chez Apple
    - http://www.securityevaluators.com/iphone/
  - Téléphone débloqué par le port JTAG
    - http://iphonejtag.blogspot.com/2007/08/step-1.html
  - La sortie très médiatique de l'iPhone a aussi été l'occasion de grandes campagnes de phishing !

Dernières vulnérabilités Histoires (4/4)

- La saga Wikipedia
  - Nouvel outil : Wikiscanner
    - http://wikiscanner.virgil.gr/
  - Les premiers résultats
    - http://wired.reddit.com/wikidgame/
    - http://www.cyberpresse.ca/article/20070817/CPACTUALITES/708170384/1019/CPACTUALITES
  - La fiabilité de Wikipedia mise en doute
    - http://www.zdnet.fr/actualites/internet/0,39020774,39371196,00.htm

Dernières vulnérabilités
Autres infos (1/3)

- **Fusions et acquisitions**
  - **Citrix achète XenSource**
  - **VMWare achète Determina**
    - **http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1268544,00.html**
  - **SourceFire achète ClamAV**
    - **http://isc.sans.org/diary.php?storyid=3276**

Dernières vulnérabilités
Autres infos (2/3)

- DefCon et BlackHat USA 2007
  - Halvar Flake interdit de séjour aux USA
    - http://www.jailhalvar.com/
  - Les lecteurs de passeport électronique affectés par une faille JPEG
    - http://www.engadget.com/2007/08/01/hackers-crash-e-passport-readers-ready-to-develop-exploits/
  - BluePill sort du bois
    - La réponse de Joanna à Matasano
      - http://bluepillproject.org/
    - McAfee pense pouvoir le détecter
      - http://www.avertlabs.com/research/blog/index.php/2007/08/13/the-truths-and-myths-about-blue-pill-and-virtualized-malware/
  - Le sniffing BlueTooth : ça progresse
    - http://www.zoller.lu/
  - Une journaliste de NBC s'enfuit de DefCon
    - http://www.youtube.com/watch?v=nCvmkxO5hoQ
    - http://blog.wired.com/27bstroke6/2007/08/media-mole-at-d.html

Dernières vulnérabilités
Autres infos (3/3)

- Et pendant ce temps là sur la mailing liste de l'OSSIR
  - Liste SUR
    - La vie des "0day"
    - "DNS Pinning"
    - Security-challenge.com
    - Virus non détecté
    - Spam DOC
    - Evènement "Global Security Week"
    - Configuration sudo
    - Loi anti-hacking en Allemagne
    - Recherche automatique et exploitation de failles Web
    - Analyse de logs
  - Liste NT
    - Automatiser la configuration de Flash Player

Questions / réponses

- Questions / réponses
- Date de la prochaine réunion
  - Prochaine réunion le 8 octobre 2007
- N'hésitez pas à proposer des sujets et des salles