OSSIR
Groupe Paris

Réunion du 13 avril 2010

Revue des dernières vulnérabilités

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

Avis Microsoft (1/20)

- **Correctifs de Février 2009**
  - **13 bulletins, 26 failles**
  - **Avec [exploitability index]**
    - **http://blogs.technet.com/srd/archive/2010/02/09/assessing-the-risk-of-the-february-security-bulletins.aspx**
  - **MS10-003 Vulnérabilité dans Office [1]**
    - **Affecte: Office XP SP3, Office 2004 pour Mac**
    - **Exploit: exécution de code à l'ouverture d'un document Office malformé**
      - **Buffer overflow dans MSO.DLL**
    - **Crédit: Damian Frizza / Core Security**
      - **http://www.coresecurity.com/content/excel-buffer-overflow**

Avis Microsoft (2/20)

- MS10-004 Vulnérabilités dans PowerPoint (x6) [2,1,1,1,1,1]
  - Affecte: Office XP SP3, Office 2003 SP3, Office 2004 pour Mac
  - Exploit: exécution de code à l'ouverture d'un fichier malformé
    - Buffer overflow, use after free, array out of bound, etc.
  - Crédit:
    - Carsten Eiram / Secunia
      - http://secunia.com/secunia_research/2009-28/
    - Sean Larsson / iDefense (x3)
      - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=840
      - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=841
      - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=842
    - SkD / ZDI
      - http://www.zerodayinitiative.com/advisories/ZDI-10-017/
    - Cody Pierce / TippingPoint DVLabs
      - http://dvlabs.tippingpoint.com/advisory/TPTI-10-02

Avis Microsoft (3/20)

- MS10-005 Vulnérabilité dans Paint [2]
  - Affecte: Windows 2000 SP4, Windows XP SP2/SP3, Windows 2003
  - Exploit: exécution de code à l'ouverture d'un fichier JPEG malformé
    - Integer overflow dans le décodeur JPEG
  - Crédit:
    - Tielei Wang / ICST-ERCIS + Secunia

Avis Microsoft (4/20)

- MS10-006 Vulnérabilités dans le client SMB (x2) [2,1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: exécution de code ou déni de service
    - Pool overflow (noyau)
    - Race condition
  - Crédit:
    - Laurent Gaffié / stratsec (& Renaud Feil)
  - Voir aussi:
    - http://seclists.org/fulldisclosure/2010/Feb/168
    - http://www.stratsec.net/files/SS-2010-003-stratsec-Microsoft-SMB-Heap-Overflow-Security-Advisory-v1.0.pdf
    - http://blogs.technet.com/srd/archive/2010/02/09/ms10-006-and-ms10-012-smb-security-bulletins.aspx
    - http://g-laurent.blogspot.com/2010/02/more-details-on-ms10-006.html

Avis Microsoft (5/20)

- MS10-007 Vulnérabilité dans ShellExecute() [1]
  - Affecte: Windows 2000 SP4, Windows XP SP2/SP3, Windows 2003
  - Exploit: validation insuffisante des paramètres passés à l'API ShellExecute()
    - ... conduisant à l'exécution de commandes
    - http://www.zerodayinitiative.com/advisories/ZDI-10-016/
    - http://blogs.technet.com/srd/archive/2010/02/09/ms10-007-additional-information-and-recommendations-for-developers.aspx
  - Crédit:
    - Brett Moore / ZDI
    - Lostmon Lords

Avis Microsoft (6/20)

- MS10-008 Mise à jour des "killbits" [-]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: failles trouvées dans ...
    - Microsoft Data Analyzer
    - Symantec WinFax Pro 10.3
    - Google Desktop Gadget 5.8
    - Facebook Photo Updater 5.5.8
    - Panda ActiveScan Installer 2.0
  - Crédit:
    - Shaun Colley / NGS Software

Avis Microsoft (7/20)

- MS10-009 Vulnérabilités dans le support IPv6 (x4) [2,2,2,3]
  - Affecte: Windows Vista & 2008 "R1"
  - Exploit: exécution de code à distance ou déni de service via des paquets malformés
    - ICMPv6 Router Advertisement
    - Fragments ESP (IPSEC)
    - ICMPv6 Route Information
    - TCP SACK
  - Crédit:
    - Sumit Gwalani, Drew Hintz, Neel Mehta / Google (x3)

Avis Microsoft (8/20)

- MS10-010 Vulnérabilité dans Hyper-V [3]
  - Affecte: Windows 2008 R1 et R2 (avec Hyper-V)
  - Exploit: déni de service sur l'hyperviseur depuis un système invité
  - Crédit:
    - Jan Bottorff

- MS10-011 Vulnérabilité dans CSRSS [1]
  - Affecte: Windows 2000 SP4, Windows XP SP2/SP3, Windows 2003
  - Exploit: élévation de privilèges locale
  - Crédit:
    - Matthew 'j00ru' Jurczyk & Gynvael Coldwind / Hispasec

Avis Microsoft (9/20)

- MS10-012 Vulnérabilités dans le serveur SMB (x4) [2,2,3,1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit:
    - Déni(s) de service (corruption mémoire, pointeur NULL)
    - Manque d'entropie dans le générateur d'aléa
  - Crédit:
    - Joshua Morin / Codenomicon
    - Florian Rienhardt / BSI
    - Hernan Ochoa
      - http://www.hexale.org/advisories/OCHOA-2010-0209.txt

- MS10-013 Vulnérabilité dans DirectShow [1]
  - Affecte: Windows (DirectX) toutes versions supportées
  - Exploit: exécution de code à l'ouverture d'un fichier malformé
    - Heap overflow dans QUARTZ.DLL à l'ouverture d'un fichier AVI
    - http://www.zerodayinitiative.com/advisories/ZDI-10-015/
  - Crédit:
    - Anonymous / ZDI

Avis Microsoft (10/20)

- MS10-014 Vulnérabilité dans Kerberos [3]
  - Affecte: Windows 2000 SP4, Windows 2003 SP2, Windows 2008 "R1"
  - Exploit: déni de service
    - Déréférencement de pointeur NULL lors du renouvellement du TGT par un client tiers n'appartenant pas au domaine Windows
  - Crédit: n/d

Avis Microsoft (11/20)

- MS10-015 Vulnérabilités dans le noyau Windows (x2) [1,2]
  - Affecte: Windows (toutes versions supportées)
    - Sauf Windows Seven x64, Windows 2008 R2 x64 et Windows 2008 R2 ia64
  - Exploit: élévation de privilèges locale
    - Problème dans le gestionnaire d'exceptions
      - (Corrige la faille "NTVDM")
    - Double free
  - Crédit:
    - Tavis Ormandy / Google
  - Note: quelques effets de bord détectés ...
    - http://blogs.technet.com/msrc/archive/2010/02/11/restart-issues-after-installing-ms10-015.aspx
  - ... sur des machines infectées !
    - http://blogs.technet.com/msrc/archive/2010/02/12/update-restart-issues-after-installing-ms10-015.aspx
    - http://blogs.technet.com/msrc/archive/2010/02/17/update-restart-issues-after-installing-ms10-015-and-the-alureon-rootkit.aspx
    - http://www.prevx.com/blog/143/BSOD-after-MS-TDL-authors-apologize.html
    - http://blogs.technet.com/msrc/archive/2010/03/02/update-ms10-015-security-update-re-released-with-new-detection-logic.aspx

Avis Microsoft (12/20)

- **Correctifs de Mars 2009**
  - **2 bulletins, 8 failles**
  - **Avec [exploitability index]**
    - **http://blogs.technet.com/msrc/archive/2010/03/09/march-2010-security-bulletin-release.aspx**
  - **MS10-016 Vulnérabilité dans Windows Movie Maker [1]**
    - **Affecte: Windows Movie Maker (Windows XP / Vista / Seven)**
      - **Microsoft Producer 2003 est également vulnérable ... et non corrigé**
    - **Exploit: exécution de code à l'ouverture d'un fichier ".mswmm" malformé**
    - **Crédit: Damián Frizza / Core SDI**
      - **http://www.coresecurity.com/content/movie-maker-heap-overflow**

Avis Microsoft (13/20)

- MS10-017 Vulnérabilités dans Excel (x7) [1,2,1,1,2,1,1]
  - Affecte:
    - Excel (toutes versions supportées, y compris Viewer et Mac OS)
    - SharePoint 2007
  - Exploit: exécution de code à l'ouverture d'un fichier Excel malformé
  - Crédit:
    - Nicolas Joly / VUPEN
    - Sean Larsson / iDefense (x4)
      - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=859
      - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=860
      - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=861
      - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=862
    - Anonymous / ZDI
      - http://www.zerodayinitiative.com/advisories/ZDI-10-025/
    - Damián Frizza / Core SDI
      - http://www.coresecurity.com/content/CORE-2009-1103

Avis Microsoft (14/20)

- **Correctif "out of band" du 30 mars 2010**
  - **MS10-018 Correctif cumulatif pour IE**
    - **Affecte: IE 5.01, IE6, IE7, IE8**
    - **Exploit: documenté dans Q981374 (et exploité dans la nature)**
      - **+ 9 autres failles corrigées (!)**
        - **http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=864**
        - **ZDI-10-033, ZDI-10-034**
    - **Crédit:**
      - **Secunia**
      - **Daiki Fukumori / Cyber Defense Institute**
      - **Alexander Kornbrust / Red Database Security**
      - **Ivan Fratric / iSight Partners**
      - **Wushi / Team509 (via iDefense)**
      - **Simon Zuckerbraun (via ZDI)**
      - **Paul Stone / Context Information Security**
      - **Anonymous (via ZDI)**
      - **ADLab / VenusTech (x2)**

Avis Microsoft (15/20)

- **Prévisions pour Avril 2010**
  - **11 bulletins**
  - **25 failles**
  - **Produits affectés: Windows, Office et Exchange**
  - **Vont être corrigés également:**
    - **Q981169 (*Vulnerability in VBScript Could Allow Remote Code Execution*)**
    - **Q977544 (*Vulnerability in SMB Could Allow Denial of Service*)**

Avis Microsoft (16/20)

- Advisories
  - Q973811 "Extended Protection for Authentication" (EPA)
    - V1.3: IIS peut désormais utiliser cette fonction
      - http://support.microsoft.com/kb/973917
  - Q977377 "Spoofing sur TLS/SSL"
    - Il s'agit de la faille de l'été 2009
    - IIS 6.0 et ultérieurs ne sont pas vulnérables
      - Sauf en cas d'authentification mutuelle
    - Un correctif pour SCHANNEL.DLL permet de désactiver la renégociation
      - http://support.microsoft.com/kb/977377
      - Mais des effets de bord ont déjà été documentés
    - Voir aussi
      - http://blogs.technet.com/srd/archive/2010/02/09/details-on-the-new-tls-advisory.aspx

Avis Microsoft (17/20)

- Q979682 Faille "NTVDM"
  - V2.0: sortie d'un correctif
- Q980088 Faille dans IE
  - (Permettant de lire n'importe quel fichier du disque dur)
  - V1.1: précisions sur le "mode protégé" dans IE
- Q981169 Faille(s) dans win32hlp
  - (Exploitable via Internet Explorer)
  - Exploitation: l'utilisateur doit appuyer sur "F1" au moment où une boite de dialogue s'affiche
  - Références:
    - http://isec.pl/vulnerabilities/isec-0027-msgbox-helpfile-ie.txt
    - http://blogs.technet.com/msrc/archive/2010/02/28/investigating-a-new-win32hlp-and-internet-explorer-issue.aspx
    - http://blogs.technet.com/srd/archive/2010/03/01/help-keypress-vulnerability-in-vbscript-enabling-remote-code-execution.aspx

Avis Microsoft (18/20)

- Q981374 Faille dans Internet Explorer 6 et 7
  - Exploitée en "0day"
    - http://www.rec-sec.com/2010/03/10/internet-explorer-iepeers-use-after-free-exploit/
  - Contournement: bloquer "iepeers.dll"
    - http://blogs.technet.com/msrc/archive/2010/03/09/security-advisory-981374-released.aspx
    - Attention aux effets de bord (impression, Web folders, ...)
  - V1.1: désactiver le composant "Peer Factory"
  - V1.2: publication d'un "Fix It"
  - V2.0: corrigé par MS10-018

Avis Microsoft (19/20)

- **Révisions**
  - **MS09-033**
    - **V2.0: Virtual Server 2005 est également affecté**
  - **MS09-060**
    - **V1.4: changement dans la logique de détection du patch**
  - **MS10-002**
    - **V1.2: correction du niveau de risque pour IE 6 sur Windows XP; mise à jour de la FAQ**
    - **V1.3: correction du niveau de risque pour IE 5 sur Windows 2000 et IE 6 sur Windows XP**
  - **MS10-003**
    - **V1.1: ajout d'un problème connu (Q978214)**
  - **MS10-005**
    - **V1.1: correction du nom de la clé de BdR sous Windows XP 64 bits; un redémarrage n'est pas toujours nécessaire**
  - **MS10-006**
    - **V1.1: correction pour le déploiement à travers SMS 2003**
  - **MS10-008**
    - **V1.1: correction pour le déploiement à travers SMS 2003; correction sur le statut par défaut du contrôle ActiveX**

Avis Microsoft (20/20)

- MS10-009
  - V1.1: correction du workaround (règle de filtrage)
- MS10-010
  - V1.1: correction pour le déploiement à travers SMS 2003
- MS10-011
  - V1.1: correction du nom de la clé de BdR sous Windows XP 64 bits
- MS10-012
  - V1.1: nombreuses corrections documentaires
- MS10-013
  - V1.1: nombreuses corrections documentaires
- MS10-015
  - V1.1: correction du nom de la clé de BdR sous Windows XP 64 bits
  - V1.2: mise à jour de la FAQ
  - V1.3: corrections documentaires
- MS10-016
  - V1.1: correction sur les clés de BdR
- MS10-017
  - V1.1: corrections typographiques

Infos Microsoft

- **Sorties logicielles**
  - **Visual Studio 2010 et .NET 4.0 en version finale (12 avril 2010)**
  - **Premières images de Windows Phone 7**
    - **http://www.youtube.com/watch?v=Z5ilUZNLZhs**
  - **Virtualisation sous Seven sans support matériel**
    - **http://support.microsoft.com/kb/977206**
  - **SDL, version 5**
    - **http://blogs.msdn.com/sdl/archive/2010/04/01/now-available-sdl-process-guidance-version-5.aspx**
  - **Le téléphone à traduction instantanée**
    - **(Beta)**
      - **http://gizmodo.com/5483358/microsofts-translating-telephone-the-realtime-translator-we-assumed-wed-have-by-now**

Infos Microsoft

- Autre
  - Fin du support pour Vista RTM
    - 13 avril 2010
  - L'écran de choix d'un navigateur alternatif poussé au travers de Windows Update
    - Une exigence de la commission européenne
      - http://www.browserchoice.eu/BrowserChoice/browserchoice_fr.htm
  - L'enterrement d'IE6
    - http://ie6funeral.com/
  - Les premières versions d'IE9 disponibles
    - http://ie.microsoft.com/testdrive/info/ThankYou/Default.html

Infos Microsoft

- Microsoft Security Response sur Twitter
  - http://twitter.com/msftsecresponse
- Version finale du "*Security Compliance Manager*"
  - http://technet.microsoft.com/en-us/library/cc677002.aspx
- Le "Global Criminal Compliance Handbook" s'égare ...
  - Et Microsoft fait fermer Cryptome.org pour le "récupérer" !
    - http://www.theregister.co.uk/2010/02/25/cryptome_dmca_takedown/
- Microsoft 1 – Waledac 0
  - http://blogs.technet.com/microsoft_blog/archive/2010/02/25/cracking-down-on-botnets.aspx
- Un accord Microsoft - Yahoo! en perspective (?)

Infos Microsoft

- Encore un certificat expiré dans la solution RMS
  - 22 février 2010
    - http://blogs.msdn.com/rms/archive/2010/02/09/required-critical-update-for-ad-rms-customers.aspx
- Microsoft lance la traque des Windows Seven piratés
    - http://arstechnica.com/microsoft/news/2010/02/new-windows-7-antipiracy-update-to-phone-home-regularly.ars
- Le Poitou-Charentes, repaire de pirates
    - http://www.infos-du-net.com/actualite/16650-microsoft-piratage-poitou-charentes.html
- Microsoft et les blagues "pas drôles" du 1er avril
    - http://www.numerama.com/magazine/15407-pour-le-1er-avril-microsoft-fait-une-lecon-de-morale-aux-pirates-qui-s-amusent.html

Infos Réseau

- **Principales failles**
  - **Cisco IronPort**
    - **Accès distant anonyme au système de fichiers, exécution de code distante anonyme ... (CVSS = 10)**
      - **La faille était dans la config JBoss**
      - **http://www.cisco.com/warp/public/707/cisco-sa-20100210-ironport.shtml**
  - **Cisco ASA**
    - **Contournement de l'authentification (si NTLMv1 est utilisé)**
      - **http://www.cisco.com/warp/public/707/cisco-sa-20100217-asa.shtml**
    - **Et plein d'autres """DoS"""**
      - **TCP, SIP, SCCP, DTLS, IKE, ...**

Infos Réseau

- Les bulletins Cisco "classiques"
  - 7 failles pour ce semestre
    - http://www.cisco.com/en/US/products/products_security_advisories_listing.html
  - Vecteurs:
    - Protocole IKE sur Cisco 7200/7300
    - Protocole SCCP sur Cisco IOS
      - Pré-requis: Cisco CME ou Cisco SRST activé
    - Protocole SCCP sur Cisco IOS
      - Pré-requis: NAT + fragmentation SCCP
    - Protocole H.323 sur Cisco IOS
    - Protocole SIP sur Cisco IOS
    - Protocole MPLS sur Cisco IOS
    - Protocole TCP sur Cisco IOS
      - Pré-requis: TCP window size forcée, PMTUD, SNAT

Infos Réseau

- BIND 9.6.2
  - http://isc.org/files/release-notes/962.html
- Nouvelles attaques sur TKIP
  - Utilisation de la fragmentation IP & collision de MIC
    - Pour récupérer plus de keystream, plus rapidement
  - Astucieux ... et presque dangereux
    - http://download.aircrack-ng.org/wiki-files/doc/enhanced_tkip_michael.pdf
- Un buffer overflow exploitable dans Aircrack (!)
  - http://code.google.com/p/pyrit/source/detail?r=239
- H.D. Moore vs. NTP
  - http://www.sensepost.com/blog/4552.html

Infos Réseau

- Autres infos
  - Cisco abandonne le WiMax
    - http://www.engadget.com/2010/03/08/another-one-bites-the-dust-cisco-steps-out-of-the-wimax-game/
  - Cisco change sa politique de publication des correctifs
    - Nouvelles dates: les quatrièmes mercredis des mois de mars et septembre
  - 50.0.0.0/8 et 107.0.0.0/8 alloués
  - Une liste de Bogons à jour
    - http://www.team-cymru.org/Services/Bogons/
  - Encore un problème BGP
    - Cette fois-ci dû à un opérateur chinois
      - http://bgpmon.net/blog/?p=282

Infos Réseau

- Le botnet "Chuck Norris" infecte les modems ADSL non sécurisés
  - http://www.pcworld.idg.com.au/article/336938/chuck_norris_botnet_karate-chops_routers_hard/
- L'AFNIC passe à DNSSEC
  - La racine ".fr" sera signée d'ici juillet 2010
    - http://www.afnic.fr/afnic/r_d/dnssec
- Le ".YU" (Yougoslavie) remplacé par le ".RS" (Serbie)
- Canon aura-t-il son ".canon" ?
  - http://www.clubic.com/actualite-330710-canon-nom-domaine.html

Infos Réseau

- Un outil d'analyse des règles de filtrage Cisco
  - http://runplaybook.com/p/11
- YouTube passe en IPv6
  - http://youtube-global.blogspot.com/2010/02/youtube-calls-on-ipv6.html
- NAT64 et DNS64 pour IPv6
  - http://www.viagenie.ca/news/index.html#nat64_dns64_announce

Infos Unix

- (Principales) failles
  - Screen Saver EPIC FAIL
    - Il suffit d'appuyer sur la touche "Entrée" pour le faire planter
    - Gnome:
      - http://permalink.gmane.org/gmane.comp.security.oss.general/2588
    - KDE:
      - http://bugs.kde.org/show_bug.cgi?id=226449
  - Screen Saver FAIL ... again
    - Il suffit d'attacher un deuxième écran
      - https://bugzilla.gnome.org/show_bug.cgi?id=593616
  - Apache.org compromis
      - https://blogs.apache.org/infra/entry/apache_org_04_09_2010

Infos Unix

- OpenSSL 0.9.8m implémente RFC 5746
  - Et corrige donc la faille de "renégociation TLS"
    - http://permalink.gmane.org/gmane.comp.encryption.openssl.announce/70
- GnuTLS (going to) FAIL ?
    - http://www.openldap.org/lists/openldap-devel/200802/msg00072.html
- Apache < 2.2.15
  - Intègre OpenSSL 0.9.8m
  - Et corrige plusieurs failles
    - http://httpd.apache.org/security/vulnerabilities_22.html
- Linux < 2.6.33-rc7
  - Fuite d'information ou DoS (local) à travers do_pages_move()
    - http://permalink.gmane.org/gmane.comp.security.oss.general/2566
- mod_security <= 2.5.11 (DoS)
  - Crédit: Sogeti/ESEC

Infos Unix

- CUPS
  - "Format string" dans lppasswd
  - Le bogue n'est pas visible publiquement sur le site d'Apple ☺
    - http://www.cups.org/str.php?L3482
- Wordpress 2.9 (< 2.9.2)
  - Il est possible de faire du "trashing" ☺
    - http://wordpress.org/development/2010/02/wordpress-2-9-2/
- Faille(s) dans KVM
    - https://rhn.redhat.com/errata/RHSA-2010-0126.html
- Faille dans "sudoedit" 1.6.9 - 1.7.2p3
    - http://www.sudo.ws/sudo/alerts/sudoedit_escalate.html
- Faille (triviale !) dans "SpamAssassin milter plugin"
  - Heureusement dans une configuration "non par défaut"
    - http://archives.neohapsis.com/archives/fulldisclosure/2010-03/0139.html

Infos Unix

- PHP < 5.2.13
  - http://www.php.net/ChangeLog-5.php#5.2.13
- PHP 6 s'arrête
  - Le support de l'Unicode est trop compliqué
    - http://news.php.net/php.internals/47120
- PHP + génération d'aléa = FAIL
  - http://svn.php.net/viewvc/php/php-src/trunk/ext/standard/lcg.c?r1=293036&r2=293253
- Debian (+ Suhosin) = FAIL
  - http://www.suspekt.org/2010/02/27/debian-breaks-suhosin-security-feature/
- Déni de service sur Squid 2.7 et 3.0
  - Via le protocole HTCP (mise en cache, RFC2756)
    - http://www.squid-cache.org/Advisories/SQUID-2010_2.txt

Infos Unix

- Failles multiples dans OpenOffice < 3.2
  - Aucun avis de l'éditeur ?
    - http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-080/CERTA-2010-AVI-080.html
  - Finalement si ...
    - http://www.openoffice.org/security/bulletin.html
    - (dont une faille LibXML2 de ... 2006)
  - Par ailleurs OpenOffice 2 est "end of life"
    - http://development.openoffice.org/releases/eol.html

Infos Unix

- **Autre**
  - **Annonces Oracle**
    - **Solaris ne sera plus gratuit**
    - **Et OpenSolaris ne contiendra plus toutes les fonctionnalités de Solaris**
  - **Création du Conseil National du Logiciel Libre**
    - **http://www.cnll.fr/**

Failles

- **Principales applications**
  - **Acrobat < 9.3.1, < 8.2.1**
    - **http://www.adobe.com/support/security/bulletins/apsb10-07.html**
    - **Une vulnérabilité issue de la LibTIFF corrigée silencieusement ...**
      - **http://secunia.com/blog/76**
    - **Cette faille date de 2006 (CVE-2006-3459) !**
      - **http://blog.metasploit.com/2010/03/latest-adobe-exploit-and-session.html**
      - **Accessoirement, c'est aussi la faille exploitée il y a quelques temps pour 'jailbreaker' l'iPhone ...**
  - **Adobe Download Manager < 1.6.2.60**
    - **Permet le téléchargement et l'exécution de fichiers arbitraires ...**
      - **http://www.adobe.com/support/security/bulletins/apsb10-08.html**
    - **Le produit est développé par la société NOS (et potentiellement utilisé par d'autres vendeurs)**
      - **http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=856**

Failles

- Flash < 10.0.45.2
  - Contournement de la Same Origin Policy
    - http://www.adobe.com/support/security/bulletins/apsb10-06.html
  - Note: Flash Player 10.1 honore le "private browsing" dans tous les navigateurs supportés
    - http://www.adobe.com/devnet/flashplayer/articles/privacy_mode_fp10.1.html
    - La fin des "super cookies" ?
- Google Chrome < 4.0.249.89
    - http://googlechromereleases.blogspot.com/2010/02/stable-channel-update.html
- Google Chrome < 4.1.249.1036
    - http://googlechromereleases.blogspot.com/2010/03/stable-channel-update.html
- Safari < 4.0.5 (et Chrome 3.x)
    - http://support.apple.com/kb/HT4070
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=863
    - ZDI-10-029, ZDI-10-030, ZDI-10-031
    - http://www.vupen.com/english/advisories/2010/0599

Failles

- Une faille non corrigée, affectant Firefox < 3.6.2, en vente dans la nature
  - Par la "fameuse" société Intevydis / VulnDisco
    - http://hackingexpose.blogspot.com/2010/02/attack-code-for-firefox-zero-day-goes.html
  - Corrigée dans la version 3.6.2 de FireFox
    - http://www.mozilla.org/security/announce/2010/mfsa2010-08.html
  - Pour certains, "seeing is believing" …
    - http://secunia.com/blog/90/
  - Le BSI (allemand) avait déconseillé l'utilisation de FireFox
    - En attendant le correctif
    - http://www.theregister.co.uk/2010/03/22/germany_firefox_warning/

Failles

- Firefox < 3.5.9, < 3.0.19
  - http://www.mozilla.org/security/known-vulnerabilities/firefox35.html
  - Attention: la branche 3.0 n'est plus officiellement maintenue
- Firefox < 3.6.3
  - http://www.mozilla.org/security/known-vulnerabilities/firefox36.html
  - Corrige la faille utilisée lors de Pwn2Own 2010
    - http://www.mozilla.org/security/announce/2010/mfsa2010-25.html
- Voir aussi
  - ZDI-10-019, ZDI-10-046, ZDI-10-047, ZDI-10-048 ZDI-10-049, ZDI-10-050

Failles

- Opera 10.5
  - Des failles corrigées ?
    - http://www.opera.com/docs/changelogs/windows/1050/
  - Et des failles non corrigées
    - http://secunia.com/advisories/38820/
- Opera < 10.51
    - http://www.opera.com/support/kb/view/948/
    - http://www.opera.com/support/kb/view/949/
    - http://www.opera.com/docs/changelogs/windows/1051/
- ThunderBird < 3.0.4

Failles

- Java < 1.6.19, < 1.5.24, < 1.4.2_26
  - http://www.oracle.com/technology/deploy/security/critical-patch-updates/javacpumar2010.html
  - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=865
  - http://secunia.com/secunia_research/2009-49/
  - http://secunia.com/secunia_research/2009-50/
  - Ainsi que ZDI-10-051, ZDI-10-052, ZDI-10-053, ZDI-10-054, ZDI-10-055, ZDI-10-056, ZDI-10-057, ZDI-10-059, ZDI-10-060, ZDI-10-061
  - Note: ces failles sont extrêmement critiques !
    - Exécution de code Java dans un contexte privilégié
- Faille critique, non corrigée, Java
  - En cause: l'intégration Java Web Start dans le navigateur
    - http://seclists.org/fulldisclosure/2010/Apr/119
    - http://blog.cr0.org/2010/04/javacalypse.html

Failles

- iTunes < 9.1
  - http://support.apple.com/kb/HT4105
- QuickTime < 7.6.6
  - http://support.apple.com/kb/HT4104
  - Voir aussi
    - ZDI-10-035, ZDI-10-036, ZDI-10-037, ZDI-10-038, ZDI-10-040, ZDI-10-041, ZDI-10-042, ZDI-10-043, ZDI-10-044, ZDI-10-045, ZDI-10-067, ZDI-10-068
- Mac OS X < 10.6.3
  - 800 Mo de mises à jour (!)
    - http://support.apple.com/kb/HT1222
    - http://support.apple.com/kb/HT4077
    - http://support.apple.com/kb/HT4014
    - http://support.apple.com/kb/HT4015
  - Voir aussi
    - ZDI-10-039, ZDI-10-058
  - Dont une faille Xterm de 2003 …
    - CVE-2003-0063

Failles

- (Redécouverte) de la faille "Launch Action" dans le format PDF
  - Et la réponse d'Adobe
    - http://blogs.adobe.com/adobereader/2010/04/didier_stevens_launch_function.html
- Le Top 25 des failles les plus courantes (en 2010)
  - #1 XSS
  - #2 SQL injection
  - #3 buffer overflow
    - http://cwe.mitre.org/top25/

Failles

- Faille dans Autonomy KeyView
  - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=858
  - Affecte forcément de nombreux produits tiers
    - Lotus Notes, Symantec, ...
- Faille dans le firmware des cartes réseau HP/Broadcom
  - Permettant l'exécution de code à distance
    - CVSS = 10.0
    - Cf. conférence CanSecWest 2010
    - http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02048471
- Real Player (failles du mois de janvier)
  - http://service.real.com/realplayer/security/01192010_player/fr/

Failles 2.0

- Récit d'une intrusion ciblée
  - A l'aide des réseaux sociaux
    - http://www.usatoday.com/tech/news/computersecurity/2010-03-04-1Anetsecurity04_CV_N.htm?csp=hf
- "Shadows In The Cloud"
  - Enquête sur des intrusions
    - http://www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0
- "Hacker Croll" arrêté à Clermont-Ferrand
  - Il avait "piraté" Twitter en devinant des mots de passe
    - http://www.zataz.com/news/20044/hacker-croll--hackercroll--hacker-croll.html
- Un PC Windows équipé d'applications "standard" doit être patché
  - ... tous les 5 jours en moyenne !
    - http://www.infoworld.com/d/security-central/typical-windows-user-patches-every-5-days-630

Malwares et spam

- Un antivirus matériel ?
  - S'insère sur la nappe du disque dur
    - http://gizmodo.com/5473196/patent-for-hardware-antivirus-device-granted-to-russian-inventor
- Un téléphone HTC Magic infecté en usine
    - http://research.pandasecurity.com/vodafone-distributes-mariposa/
  - Par ailleurs le botnet Mariposa est un cas d'étude intéressant
    - D'autant que le botmaster a été arrêté en Espagne il y a peu
    - http://pandalabs.pandasecurity.com/mariposa-botnet/
- En 2009, 80% des attaques viennent par un PDF
    - http://www.computerworld.com/s/article/9157438/Rogue_PDFs_account_for_80_of_all_exploits_says_researcher
- Un support technique payant
  - ... pour un rogue antivirus
    - http://www.networkworld.com/news/2010/021310-rogue-antivirus-program-comes-with.html
- Les antivirus efficaces dans moins de 30% des attaques "réelles"
    - http://www.cyveillance.com/web/forms/request.asp?getFile=116

Malwares et spam

- Un malware signé par une vraie-fausse CA "Verisign"
  - http://www.cccure.org/article-topic-42.html
- Un malware qui propage ses liens via Skype IM
  - http://cert.at/static/downloads/papers/cert.at-an_analysis_of_the_skype_imbot_logic_and_functionality_1.2.pdf
- Un ver infecte plus de 250,000 pages sur Facebook
  - http://securitylabs.websense.com/content/Blogs/3579.aspx
- Antivirus (*badly*) FAIL
  - http://krebsonsecurity.com/2010/04/trendmicro-toolbar-long-url-fail/
- Un *botnet* de recherche sur téléphones mobiles
  - 8000 téléphones sous contrôle
    - http://www.darkreading.com/insiderthreat/security/client/showArticle.jhtml?articleID=223200001

Malwares et spam

- Le CD "compagnon" d'un chargeur de piles infectés
  - … depuis au moins 3 ans
  - … par un Cheval de Troie trivial (bind & execute)
  - … module d'exploitation disponible dans Metasploit
    - http://www.01net.com/editorial/513713/un-chargeur-de-piles-usb-energizer-abrite-un-cheval-de-troie/
    - http://www.mobilemag.com/2010/03/08/energizers-duo-usb-charger-is-infected-with-a-trojan-virus/

Actualité (francophone)

- Bro 1.4 certifié CSPN
  - http://www.ssi.gouv.fr/site_rubrique54_certificat_cspn_2009_06.html
- Création d'un centre de lutte contre les attaques informatiques
  - Sous direction de l'ANSSI
    - http://www.journaldunet.com/solutions/breve/france/45952/centre-de-lutte-contre-les-attaques-it---la-mise-en--uvre-est-lancee.shtml
- Le site http://www.econumerique.pme.gouv.fr/ défacé
  - http://www.zataz.com/news/19966/Eymz--WaZo--deface--site-owned.html
- La boite mail de deux députés trivialement piratée
  - "J'ai perdu mon mot de passe"
    - http://www.rue89.com/2010/03/12/comment-un-hacker-a-penetre-la-boite-mail-de-deux-deputes-142539
  - La réponse de l'intéressé
    - http://www.numerama.com/magazine/15268-pirate-le-depute-philippe-goujon-porte-plainte-mais-prend-ses-electeurs-pour-des-imbeciles.html

Actualité (francophone)

- La création de l'ARJEL s'accélère
  - http://wearesecure.blogspot.com/2010/04/larjel-votee-aujourdhui.html
- Ca barde pour la SNCF
  - Page "bizarre" apparue sur leur site
  - Faille critique sur le site "voyages-sncf.com"
    - http://www.lemonde.fr/societe/article/2010/03/17/les-coordonnees-de-millions-de-clients-de-la-sncf-disponibles-sur-le-net_1320321_3224.html
  - Contrôle de la CNIL
    - http://twitter.com/CNIL/status/10678595161

Actualité (francophone)

- "Le" site de vente de détecteurs de radars n'a pas été piraté
  - http://www.numerama.com/magazine/15339-detecteurs-de-radars-pas-de-hack-par-la-gendarmerie.html
  - Plusieurs grands médias ont fait un raccourci un peu rapide …
    - Ex. Le Monde, le Figaro …
    - http://www.lemonde.fr/societe/article/2010/03/24/les-possesseurs-de-detecteurs-de-radars-dans-la-ligne-de-mire_1323601_3224.html
- Du côté de la loi …
  - La LOPPSI adoptée
    - http://www.linformaticien.com/Actualit%C3%A9s/tabid/58/newsid496/7807/la-loi-loppsi-adoptee-a-l-assemblee-nationale/Default.aspx
  - L'adresse IP devient une donnée personnelle
  - Le CIL devient obligatoire dans les entreprises de plus de 100 personnes
  - Les pertes de données devront être notifiées à la CNIL et aux victimes
    - http://www.pcinpact.com/actu/news/55567-cnil-defaut-securisation-donnees-adresse.htm
    - http://www.zdnet.fr/actualites/internet/0,39020774,39750389,00.htm
- L'armée française face aux réseau sociaux
  - Pas d'interdiction particulière
    - http://www.zdnet.fr/actualites/internet/0,39020774,39713622,00.htm

Actualité (francophone)

- Over-Blog attaqué par un DDoS de grande ampleur
  - Etaient visés: des blogs s'opposant à la Franc-Maçonnerie
    - http://www.itespresso.fr/securite-it-over-blog-subit-une-attaque-de-grande-ampleur-34355.htmlEN.pdf
- La Suisse lance SuisseID
    - http://www.kmu.admin.ch/suisseid/index.html?lang=fr
- Qu'est-ce que la "quasi neutralité" ?
    - http://www.zdnet.fr/blogs/infra-net/incroyable-l-arcep-invente-la-quasineutralite-des-reseaux-39713475.htm
- France Telecom recrute ...
  - ... Christine Albanel
    - http://www.lefigaro.fr/societes/2010/02/19/04015-20100219ARTFIG00559-christine-albanel-rejoint-france-telecom-.php

Actualité (anglo-saxonne)

- L'exercice "Cyber Shockwave" fait couler de l'encre
  - Site officiel
    - http://www.bipartisanpolicy.org/news/press-releases/2010/02/cyber-shockwave-shows-us-unprepared-cyber-threats
  - Est-ce réaliste ? Est-ce significatif ?
    - http://isc.sans.org/diary.html?storyid=8272
    - http://taosecurity.blogspot.com/2010/02/reaction-to-cyber-shockwave.html
- Secunia intègre "PSI" avec Microsoft WSUS et Microsoft SCCM
  - Dans la version CSI (Corporate Software Inspector) 4.0
    - http://secunia.com/blog/91/
- SecurityFocus devient "Symantec Connect"
  - Seule la liste "Bugtraq" et le portail des vulnérabilités subsistent
    - http://www.securityfocus.com/news/11582

Actualité (anglo-saxonne)

- Vers des obligations de sécurité pour les éditeurs de logiciels ?
  - Une initiative du SANS, du MITRE, et de plusieurs éditeurs …
    - http://www.sans.org/appseccontract/
- Pour un meilleur respect de la vie privée aux USA
  - Soutiens: AOL, Google, Microsoft ...
    - http://www.digitaldueprocess.org/
- L'Angleterre met en place un HADOPI-*like*
    - http://www.pcworld.fr/2010/04/09/internet/piratage-angleterre-desormais-son-hadopi/484121/
- Apple récupère Window Snyder
    - http://threatpost.com/en_us/blogs/apple-snags-former-mozilla-security-chief-030210
- Intel visé par l'opération "Aurora" (?)
    - http://www.zdnet.fr/actualites/informatique/0,39040745,39713306,00.htm

Actualité (européenne)

- Allemagne vs. Facebook
  - http://www.cidal.diplo.de/Vertretung/cidal/fr/__PR/actualites/nq/2010__04/2010__04__07__Aigner__Facebook__pm.html
- Les parlementaires européens contre ACTA
  - http://www.pcinpact.com/actu/news/55783-acta-resolution-parlement-europeen-acac.htm
- Premier "Permanent Stakeholders' Group" (PSG) de l'ENISA
  - Seuls 2 français sur 30 membres ?
    - http://www.enisa.europa.eu/about-enisa/structure-organization/psg/members
    - http://www.enisa.europa.eu/media/press-releases/fr-new-psg-press-release

Actualité (Google)

- Google Buzz
  - Quelques jours d'existence et déjà des inquiétudes
    - http://www.businessinsider.com/warning-google-buzz-has-a-huge-privacy-flaw-2010-2
  - Une plainte déposée aux USA
    - http://www.lemonde.fr/technologies/article/2010/02/17/une-plainte-deposee-contre-google-buzz-aux-etats-unis_1307212_651865.html
- Google quitte la Chine pour Hong Kong
  - Affaire à suivre …
    - http://www.lemonde.fr/technologies/article/2010/03/22/google-ferme-google-cn_1323002_651865.html
- Le PDG de Google Italie condamné
  - Pour une vidéo YouTube
    - http://news.bbc.co.uk/2/hi/technology/8533695.stm
- La commission européenne demande des comptes à Google
  - Pour abus de position dominante
    - http://eco.rue89.com/2010/02/24/plainte-contre-google-a-bruxelles-ils-nous-ont-envoyes-au-tapis-140253
  - En cause: le déréférencement abusif de concurrents

Actualité (crypto)

- Une attaque hardware permettant l'extraction de clés privées
  - Nécessite de moduler l'alimentation électrique du système
  - Nécessite l'implémentation OpenSSL de l'exponentiation modulaire
  - Suppose que l'unité de multiplication va être la première à "faillir"
    - http://www.eecs.umich.edu/~valeria/research/publications/DATE10RSA.pdf
    - http://rdist.root.org/2010/03/08/attacking-rsa-exponentiation-with-fault-injection/
- Le modèle de sécurité du SSL menacé par l'interception légale
    - http://www.crypto.com/blog/spycerts/
    - http://files.cloudprivacy.net/ssl-mitm.pdf
- Le modèle de sécurité du SSL est un échec
    - http://groups.google.com/group/mozilla.dev.security.policy/browse_thread/thread/b6493a285ba79998/26fca75f9aeff1dc

Actualité (crypto)

- Sortie de OpenSSL 1.0.0 (!)
- Plus de 50% des managers violent délibérément les règles de protection de leur portable
  - En particulier le chiffrement
    - http://www.cio-online.com/actualites/lire-la-principale-menace-pour-la-securite-se-situe-entre-le-clavier-et-le-siege-2783.html

Actualité

- **BlackHat DC 2010 (suite)**
  - Février 2010
    - Attaque sur les TPM
      - http://www.nzherald.co.nz/technology/news/article.cfm?c_id=5&objectid=10625082&pnum=0

- **ShmooCon 2010**
  - Février 2010
    - http://www.shmoocon.org/presentations.html
  - Des sujets originaux
    - Découvertes de données confidentielles sur les réseaux P2P
    - Attaque sur le serveur Tomcat embarqué dans l'interface d'administration VMWare
      - http://www.skullsecurity.org/blog/?p=436
    - Un logiciel d'espionnage pour BlackBerry (TXSBBspy)
    - Etc.

Actualité

- Conférence CanSecWest 2010
  - Des talks de qualité
    - http://cansecwest.com/
  - Et le concours PWN2OWN
    - Seul Chrome n'a pas été attaqué
    - … mais de nombreux correctifs avaient été publiés la semaine précédente
      - http://dvlabs.tippingpoint.com/blog/2010/02/15/pwn2own-2010
- Qubes OS
  - Le système d'exploitation "sûr" proposé par Joanna
    - http://theinvisiblethings.blogspot.com/2010/04/introducing-qubes-os.html
    - http://qubes-os.org/

Actualité

- Le produit CORE IMPACT ajoute le support des modules Metasploit
  - http://www.coresecurity.com/content/core-impact-metasploit-project
- Publication de MEHARI 2010
  - https://www.clusif.asso.fr/fr/production/ouvrages/type.asp?id=METHODES
- Publication de ISO 27003:2010
  - "Information technology -- Security techniques -- Information security management system implementation guidance"
    - http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?ics1=35&ics2=040&ics3=&csnumber=42105
- Contribuez à l'IETF (sans être membre)
  - http://iucg.org/

Fun

- $100,000 pour casser une clé USB
  - Heureusement vous ne disposez que de quelques minutes …
    - http://www.swissarmy.com/Marketing/Pages/crackthecode.aspx
- Le site officiel du film "Alvin and the Chipmunks" fermé par YouTube
  - Pour violation de copyright …
    - http://www.youtube.com/OfficialSqueakquel
- Une interview de DJB
  - "DNSSEC, *a project to cryptographically sign DNS records, has been under development for ten years by a large (and obviously rather incompetent) team of protocol developers.*"
    - http://www.aaronsw.com/weblog/001502
- L'iPad *jailbreaké* en 25h

Fun

- Un Letton pirate les banques de son pays
  - Et devient un héros national !
    - http://www.lemonde.fr/technologies/article/2010/02/25/en-lettonie-un-robin-des-bois-virtuel-defie-les-grandes-entreprises_1311419_651865.html
- Des clandestins fraudent le système biométrique japonais
  - Avec du scotch ...
    - http://search.japantimes.co.jp/cgi-bin/nn20100127f4.html
- FUDSEC en action
    - http://www.linformaticien.com/Actualit%C3%A9s/tabid/58/newsid496/7850/gigantesque-faille-dans-windows/Default.aspx

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 11 mai 2010
- N'hésitez pas à proposer des sujets et des salles