OSSIR
Groupe Paris

Réunion du 10 mars 2009

Revue des dernières vulnérabilités

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

Avis Microsoft (1/7)

- **Correctifs de Février 2009**
  - **Avec [*exploitability index*]**
  - **MS09-002 Failles multiples dans Internet Explorer (x2) [1,1]**
    - **Affecte: Internet Explorer 7**
    - **Exploit: exécution de code via une page Web malformée**
    - **Crédit: ZDI, Sam Thomas / ZDI**
    - **Note: cette faille est désormais exploitée "dans la nature"**
      - **Via un fichier XML qui s'ouvre dans Word**
      - **(permet de contourner le mode protégé d'IE sous Vista)**
      - **http://blogs.technet.com/srd/archive/2009/03/03/behavior-of-activex-controls-embedded-in-office-documents.aspx**
      - **http://isc.sans.org/diary.html?storyid=5884**
      - **http://isc.sans.org/diary.html?storyid=5899**

Avis Microsoft (2/7)

- MS09-003 Failles multiples dans Exchange (x2) [2,2]
  - Affecte: Exchange (toutes versions supportées)
    - Exchange 2003 SP1 / 2007 SP0 ne sont plus supportés
    - Cisco Unity serait affecté également
  - Exploit: exécution de code à distance (?)
    - Format TNEF malformé
    - Appel MAPI RPC malformé vers EMSMDB32
  - Crédit: Bogdan Materna / VoIP Shield

Avis Microsoft (3/7)

- MS09-004 Faille SQL Server [1]
  - Affecte:
    - SQL Server 2000 SP4 / 2005 SP2
    - Certaines versions de MSDE ou Windows Internal Database
  - Exploit: faille déjà exploitée dans la nature
    - Fonction sp_replwritetovarbin() - cf. 961040
  - Crédit: Bernhard Mueller / SEC Consult

- MS09-005 Failles multiples dans Visio (x3) [2,2,2]
  - Affecte: Visio (toutes versions supportées)
  - Exploit: exécution de code via un fichier ".vsd" malformé
  - Crédit: Bing Liu / Fortinet (x3)

Avis Microsoft (4/7)

- A noter également
  - Mises à jour WSUS
    - http://support.microsoft.com/kb/894199
  - Mises à jour "non sécurité"
    - http://technet.microsoft.com/en-us/wsus/bb466214.aspx
  - 967940: mise à jour pour corriger le comportement de la clé "NoDriveTypeAutorun"
    - A la suite de Conficker ...

- Advisories
  - 961040: Patch disponible pour la faille SQL Server
  - 960715: Mise à jour des "kill bits"
    - Akamai Download Manager
    - RIM AxLoader

Avis Microsoft (5/7)

- 968272: Faille "0day" dans Excel
  - Affecte: Excel (toutes versions supportées)
  - Exploit:
    - Attaques ciblées contre Office 2007 + Windows XP
    - http://blogs.technet.com/swi/archive/2009/02/24/more-information-about-the-new-excel-vulnerability.aspx
    - http://research.eeye.com/html/alerts/zeroday/20090224.html
    - http://www.symantec.com/security_response/writeup.jsp?docid=2009-022310-4202-99

- Prévisions pour Mars 2009
  - Pas de patch pour la faille Excel (KB968272)
  - Faille #1
    - Affecte: Windows (toutes versions supportées)
    - Exploit: exécution de code à distance (avec ou sans interaction ?)

Avis Microsoft (6/7)

- **Faille #2**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit: "spoofing" (?)**

- **Faille #3**
  - **Affecte: Windows (2003 & 2008)**
  - **Exploit: "spoofing" (?)**

Avis Microsoft (7/7)

- Révisions
  - MS08-024
    - Version 2.2: Windows 2008 "core" n'est pas affecté
  - MS08-040
    - Version 1.8: "MSDE 2000 sur Windows 2000" n'est pas affecté (n'existe pas ?)
  - MS08-070
    - Version 1.2: mise à jour de la FAQ
  - MS08-074
    - Version 2.0
  - MS08-076
    - Version 3.1: correction d'une clé de base de registre
  - MS09-002
    - Version 1.1: ajout d'un problème connu dans la FAQ
  - MS09-003
    - Version 2.0: le client MAPI intégré au serveur Exchange est aussi vulnérable
    - Version 2.1: précisions documentaires
  - MS09-004
    - Version 1.1 : mise à jour de la FAQ et changement de logique sur la détection

Infos Microsoft (1/4)

- **Sorties logicielles**
  - **Windows Seven RC1 pour le 10 avril**
    - **http://www.guwiv.com/portal/blogs/news/archive/2009/02/21/exclusif-la-sortie-de-windows-7-release-candidate-fix-233-e-au-10-avril-2009.aspx**
  - **Windows Mobile 6.5 annoncé**
    - **Entièrement tactile**
    - **Plus ergonomique (?)**
  - **Internet Explorer 8 prévu pour mars**
    - **http://www.techarp.com/showarticle.aspx?artno=621&pgno=0**
  - **Microsoft Online Services arrive en France**
    - **Avec une politique tarifaire agressive (1$!= 1€ ☺)**
    - **http://www.itrmanager.com/articles/88236/ouverture-microsoft-online-services-entreprises-europeennes-br-microsoft-positionne-force-marche-services-professionnels.html**

Infos Microsoft (2/4)

- **Autre**
  - **$250,000 sur la tête de l'auteur de Conficker**
    - **http://blogs.technet.com/msrc/archive/2009/02/12/conficker-activity-update.aspx**
  - **Une étude sur le phishing**
    - **http://research.microsoft.com/en-us/um/people/cormac/Papers/PhishingAsTragedy.pdf**
  - **Après Apple Store, Microsoft Store**
    - **http://www.itrmanager.com/articles/87451/microsoft-lance-propres-magasins.html**
  - **Un procès contre Microsoft**
    - **Object: le *downgrade* payant de Vista vers XP**
      - **http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127950**
  - **"Citrix Essentials" supporte Xen et ... Hyper-V**
  - **Des accords Microsoft – RedHat sur la virtualisation également**

Infos Microsoft (3/4)

- **Windows Seven**
  - **La mise à jour Vista -> Seven devrait être gratuite**
    - **(Pour les systèmes préinstallés en Vista)**
    - **http://www.techarp.com/showarticle.aspx?artno=609&pgno=0**
    - **Un aveu d'échec pour Vista ?**
  - **Windows Seven supporte nativement le format DivX**
    - **Ironique quand on sait que le DivX 3 était un codec MPEG-4 Microsoft ☺**
  - **Windows Seven fait peur**
    - **En cause: DRM & gestion des licences logicielles tierce partie**
      - **http://tech.slashdot.org/article.pl?sid=09/02/16/2259257**

Infos Microsoft (4/4)

- Internet Explorer pourra être désinstallé de Windows Seven
  - Jusqu'à quel point ... ?
  - (Problèmes des boites de dialogue HTML)

- Un problème plus complexe qu'il n'y parait
  - http://blogs.msdn.com/e7/archive/2009/02/18/engineering-the-windows-7-boot-animation.aspx

- Windows Seven vs. KDE 4
  - http://olylug.org/read.php?73,13757

Infos Réseau

- Encore une panne de l'Internet mondial
  - http://www.renesys.com/blog/2009/02/the-flap-heard-around-the-worl.shtml
  - http://asert.arbornetworks.com/2009/02/ahh-the-ease-of-introducing-global-routing-instability/
- Les nouveaux TLDs retardés
  - http://www.clubic.com/actualite-258658-icann-repousse-extensions-web.html
- Propagation de malwares sur les réseaux WiFi
  - Une possibilité, si la densité de points d'accès "vulnérables" est suffisante
    - http://cxnets.googlepages.com/
- Cisco communique ...
  - http://www.unjoursansreseau.com/

Infos Réseau

- **Failles Cisco**
  - **Cisco Application Control Engine (ACE)**
    - **Comptes par défaut**
    - **Déni de service par SSH et SNMP**
    - **Elévation de privilèges locale**
  - **Cisco Application Networking Manager (ANM)**
    - **Comptes par défaut**
    - **Traversée de répertoires**
  - **Cisco Unified MeetingPlace**
    - **Contournement de l'authentification côté serveur**
    - **Cross-Site Scripting**
  - **Cisco 7600 / Session Border Controller (SBC)**
    - **Crash du service par l'envoi d'un paquet malformé sur le port TCP/2000**

Infos Unix

- **Actualité**
  - **Après RedFlag Linux, Cuba Libre !**
    - **Enfin plutôt Nova Linux**
  - **MoonLight 1.0 disponible**
    - **Implémentation Linux de SilverLight**
    - **http://www.go-mono.com/moonlight/**
  - **Epoch 1234567890 a été franchi !**
    - **http://coolepochcountdown.com/**

Infos Unix

- Failles
  - ProFTPd 1.3.1 + authentification SQL = injection SQL
    - http://bugs.proftpd.org/show_bug.cgi?id=3173
  - Linux 64-bits ... sauf les UID/GID !
    - http://sourceware.org/bugzilla/show_bug.cgi?id=9706
  - Faille dans sudo 1.6.9
    - http://www.courtesan.com/sudo/alerts/group_vector.html
  - Faille dans cURL 5.11 (uniquement)
    - Honore une redirection vers "file://"
    - http://curl.haxx.se/docs/adv_20090303.html
  - Faille dans OpenBSD 4.3 et 4.4
    - Déni de service sur OpenBGP
  - Faille dans FreeBSD 7.0 et 7.1
    - Le démon "telnetd" permet de passer "root" localement
    - (Utilisation de LD_PRELOAD)

Infos Unix

- Faille dans OpenSC
  - Il était possible d'accéder à des objets privés sans authentification ...
  - http://permalink.gmane.org/gmane.comp.encryption.opensc.announce/22

- Failles dans djbdns 1.05
  - Faille #1: empoisonnement d'une entrée SOA dans le cache
    - http://www.your.org/dnscache/
    - http://marc.info/?l=djbdns&m=123420861917932
  - Faille #2: réponse AXFR trop longue permettant de corrompre le cache côté serveur
    - http://marc.info/?l=bugtraq&m=123575331312817
    - La prime de $1000 a été payée pour celui-là ☺

Infos Unix

- Faille(s) PHP
  - Affecte: PHP < 5.2.9
  - Exploit:
    - unzip, json_decode(), explode() permettent de provoquer un "déni de service"
    - imageRotate() permet de lire toute la mémoire du serveur

- Faille dans libpng
  - Affecte: libpng < 1.0.43 et 1.2.35
  - Exploit: exécution de code via un fichier PNG malformé
    - Une faille à fort potentiel ...
    - http://ovh.dl.sourceforge.net/sourceforge/libpng/libpng-1.2.34-ADVISORY.txt

Infos Unix

- **Faille dans la pile IPv6**
  - **Affecte: Solaris 10**
  - **Exploit: "déni de service"**
- **Faille dans rpc.metad**
  - **Affecte: Solaris 9 et 10**
  - **Exploit: déni de service**
- **Faille dans pppdial**
  - **Affecte: AIX 5.3 et 6.1**
  - **Exploit: *buffer overflow* exploitable localement**

Failles

- **Principales applications**
  - **Failles dans:**
    - **Flash < 10.0.22.87**
      - **http://www.adobe.com/support/security/bulletins/apsb09-01.html**
    - **WireShark < 1.0.6**
    - **Java < 1.6.12**
    - **Safari < 3.2.2**
      - **http://support.apple.com/kb/HT3438**
      - **http://support.apple.com/kb/HT3439**
    - **Firefox < 3.0.7**
    - **Opera < 9.64**
  - **Failles multiples (environ 45 :) dans Mac OS X et Java**
    - **http://support.apple.com/kb/HT3436**
    - **http://support.apple.com/kb/HT3437**
    - **http://support.apple.com/kb/HT3438**

Failles

- Faille(s) dans HP LaserJet
  - http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-058/CERTA-2009-AVI-058.html
- Failles dans les implémentations de références de SHA3 ...
  - http://blog.fortify.com/blog/fortify/2009/02/20/SHA-3-Round-1
- Quelques trolls sur les failles
  - Firefox patché plus vite qu'Internet Explorer (en moyenne)
    - http://blogs.zdnet.com/security/?p=2786
  - 92% des failles Microsoft voient leur criticité diminuer si l'utilisateur n'est pas administrateur local
    - Source: un vendeur de produit permettant de ne pas être administrateur local ☺
    - http://www.beyondtrust.com/documentation/whitePapers/wp_VulnerabilityReport.pdf

Failles

- **Acrobat Reader ...**
  - **Affecte: Acrobat 7, 8 et 9 (autres versions non supportées)**
  - **Exploit:**
    - **Décodage d'images au format JBIG2**
    - **Fonctionne avec une simple prévisualisation du fichier**
    - **Le support JavaScript n'est pas obligatoire pour exploiter cette faille**
  - **Chronologie:**
    - **Exploitée dans la nature**
    - **Confirmée par Adobe le 19 février**
    - **Connue depuis probablement plus de 2 mois**
    - **Mais pas de patch avant le 11 mars !**
      - **http://www.adobe.com/support/security/advisories/apsa09-01.html**
      - **http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-001/CERTA-2009-ALE-001.html**
      - **http://blog.metasploit.com/2009/02/best-defense-is-information.html**
      - **http://vrt-sourcefire.blogspot.com/2009/02/have-nice-weekend-pdf-love.html**
      - **http://vrt-sourcefire.blogspot.com/2009/02/homebrew-patch-for-adobe-acroreader-9.html**
  - **Remarque: d'autres lecteurs PDF décodent le JBIG2 de manière incorrecte !**
    - **http://www.foxitsoftware.com/pdf/reader/security.htm**

Malwares et spam

- McAfee "Mobile Security Report" 2009
  - http://www.mcafee.com/us/local_content/reports/mobile_security_report_2009.pdf
- Qui a bu boira
  - 75% des attaques proviennent de sites compromis
  - 20% des sites compromis l'ont déjà été par le passé
    - http://www.lightbluetouchpaper.org/2009/02/25/evil-searching/
- 4 ans de prison pour un "Bot Herder" américain
  - http://topnews.us/content/24146-botnet-spyware-creator-gets-four-year-prison-sentence
- Retrouver l'auteur d'un virus ... grâce à Google
  - http://blog.fortinet.com/flocker-virus-writers-name-found-via-google/

Failles 2.0

- Facebook supprime le "droit à l'oubli"
  - http://consumerist.com/5150175/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever
  - Mais faites-nous confiance ...
    - http://blog.facebook.com/blog.php?post=54434097130
  - Pour finalement revenir en arrière ...
    - http://edition.cnn.com/2009/TECH/02/18/facebook.reversal/index.html
- Une (nouvelle) application malveillante sur Facebook
  - Attaque en 2 temps via du SEO
    - http://www.topbreakingnewsheadlines.com/news/facebook-error-check-system-beware
- eWeek infecte ses lecteurs
  - Via les bannières publicitaires
    - http://securitylabs.websense.com/content/Alerts/3310.aspx

Failles 2.0

- Le réseau XBox Live
  - Victime et bientôt source d'attaques ?
    - http://www.silicon.fr/fr/news/2009/02/23/le_reseau_xbox_live_utilise_pour_des_attaques_dos_et_javascript__
- Une attaque en cours sur la liaison Chine/Taiwan
  - Vol de session TCP sur un équipement intermédiaire ?
    - http://archives.neohapsis.com/archives/dailydave/2009-q1/0107.html
- Sauvegarde fail
    - http://ma.gnolia.com/
- Comment H.D.Moore a géré le DDoS sur Metasploit
    - http://darkreading.com/security/attacks/showArticle.jhtml?articleID=214501208
- Metasploit en mode "Hacking as a Service"
    - http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=213401744

Actualité (France)

- Jurisprudence: l'adresse IP n'est pas une donnée nominative ?
  - http://www.alain-lambert-blog.org/index.php?2009/02/10/2541-internet-l-adresse-ip-n-est-plus-protegee-par-ouest-france
- SCTeam contraint de fermer suite à une "plainte"
  - http://scteam.canalblog.com/
- Voir ses traces en ligne (en version française)
  - http://www.tahitidocs.com/outils/traces/signature.html
- Le vol de document papier reste à la mode
  - Représente 49% des incidents de sécurité ...
    - http://www.mag-securs.com/spip.php?article12785
- Un concours pour promouvoir IPv6
  - http://concours.point6.net/

Actualité (France)

- HADOPI s'enflamme
  - Impossible de reprendre tous les liens ici
    - http://www.laquadrature.net/fr/APPEL-HADOPI-blackout-du-net-francais
    - http://securite.reseaux-telecoms.net/actualites/lire-la-commission-des-lois-durcit-la-loi-hadopi-19607.html
    - (...)
  - Pour résumer, réservez votre place en prison
    - http://www.piratesprisons.com/
- Programme de SSTIC 2009 publié
  - http://www.sstic.org/
  - Ouverture des inscriptions la semaine prochaine

Actualité (anglo-saxonne)

- La NSA prête à payer des milliards pour écouter Skype
  - Du FUD ?
    - http://www.theregister.co.uk/2009/02/12/nsa_offers_billions_for_skype_pwnage/
  - La preuve que c'est sûr: même les trafiquants de drogue l'utilisent
    - http://www.goodgearguide.com.au/article/277460/skype_calls_immunity_police_phone_tapping_threatened
  - EuroJust s'y intéresse également
    - http://www.eurojust.europa.eu/press_releases/2009/20-02-2009.htm

Actualité (anglo-saxonne)

- Les victimes d'injection SQL
  - Après Kaspersky ...
  - F-Secure
    - http://www.theregister.co.uk/2009/02/13/f_secure_hack_attack/
    - http://www.f-secure.com/weblog/archives/00001605.html
  - Symantec
    - http://hackersblog.org/2009/02/18/emeasymanteccom-vulnerabil-la-blind-sql-injection/

- Le FIRST organise un concours de "Best Practices"
  - Sujet: "la détection"
  - Deadline: 30 avril 2009
    - http://www.first.org/global/practices/

Actualité (anglo-saxonne)

- **Barack Obama veut faire de la sécurité informatique une priorité nationale**
  - **http://www.vnunet.fr/news/barack_obama_veut__faire_de_la_securite_informatique_une_priorite-2030240**
- **Kevin Mitnick : "le BlackBerry d'Obama est piratable"**
  - **On peut lire les mails qu'il envoie en SMTP sur Internet ☺**
    - **http://www.foxnews.com/story/0,2933,492705,00.html**
- **Et son hélicoptère aussi**
  - **Des données sensibles en partage sur un réseau P2P depuis un poste iranien (?!)**
    - **http://www.msnbc.msn.com/id/29447088/**

Actualité (anglo-saxonne)

- Le chef de la cyber-sécurité jette l'éponge
  - http://online.wsj.com/article/SB123638468860758145.html
- La FTC remonte les bretelles à CompGeek.com
  - En cause: des injections SQL triviales
    - http://www2.ftc.gov/os/caselist/0823113/index.shtm
- Le réseau de la FAA piraté
  - Federal Aviation Authority
    - http://www.networkworld.com/community/node/38384
- Le concept de lien hypertexte menacé ?
  - http://www.slate.fr/story/la-justice-am%C3%A9ricaine-menace-lhypertexte

Actualité (anglo-saxonne)

- **Rapport RSA / Security for Business Innovation Council**
  - **"Driving Fast and Forward: Managing Information Security for Strategic Advantage in a Tough Economy"**
    - **http://www.rsa.com/securityforinnovation/**
  - **Objectifs 2009:**
    1. **Choisir les priorités en fonction du ratio risque/impact**
    2. **Avoir du personnel multi-compétent**
    3. **Mettre en place des processus**
    4. **Mutualiser les coûts**
    5. **Externaliser avec prudence**

Actualité (anglo-saxonne)

- Conférence BlackHat Federal 2009
  - http://www.blackhat.com/html/bh-dc-09/bh-dc-09-main.html
  - Attaque sur Intel/TXT
    - http://theinvisiblethings.blogspot.com/2009/02/attacking-intel-txt-paper-and-slides.html
  - Nouvelle idée pour attaquer les IDN: abuser le caractère "/"
    - https://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf
  - Autre exemple
    - https://www.google.xn--com-edoaaaaaaaaaaaaaaaaaaaaaaaaaaa.phreedom.org/
  - Hacking de satellite (Adam Laurie)
  - Contourner l'authentification faciale
    - Un peu facile ...

Actualité (Google)

- **Nouveautés**
  - **Google Earth 5 ajoute la cartographie marine**
  - **Le trafic routier disponible sur Google Maps**
  - **Des prix à gagner pour toute faille dans NaCl**
    - **http://code.google.com/contests/nativeclient-security/**
  - **SRWare Iron, Chrome sans les spywares**
    - **http://www.srware.net/en/software_srware_iron_chrome_vs_iron.php**

Actualité

- BackTrack 4 disponible en Beta
  - http://www.remote-exploit.org/news.html
- L0phtCrack 6 disponible
  - http://www.l0phtcrack.com/
- Outil WarVOX pour le war-dialing massif
  - Auteur : H. D. Moore
    - http://warvox.org/

Actualité

- La "loi Nokia" permet aux entreprises finlandaises de surveiller l'activité électronique de leurs salariés
  - http://www.itrmanager.com/articles/88318/entreprises-finlandaises-peuvent-desormais-surveiller-ordinateurs-employes.html
- Une étude épidémiologique qui ne respecte pas vraiment l'anonymat
  - Etude MicroSim en Suède
    - http://arxiv.org/abs/0902.0901

Actualité

- MafiaBoy et le "star system"
  - http://www.it360.ca/index.php/early-bird-savings-in-effect.html
- Crise => stress => failles
  - Une étude Deloitte
    - http://www.silicon.fr/fr/news/2009/02/19/la_crise_economique_genere_du_stress_et_donc_les_risques_de_failles
- Des "hackers" auraient modifié informatiquement les quotas d'exploitation forestière en Amazonie
  - Source: GreenPeace
    - http://www.greenpeace.org.uk/blog/forests/hackers-help-destroy-amazon-rainforest-20081212
- Où est la vérité ?
  - La presse reprend Wikipedia qui justifie la presse
    - http://tech.slashdot.org/article.pl?sid=09/02/10/2211220

Fun

- Cheap crypto == no crypto
  - http://www.heise-online.co.uk/security/Cracking-budget-encryption--/features/112548
- Encore une erreur de PDF ... qui coûte cher ☺
  - http://eco.rue89.com/2009/02/13/la-bourde-qui-revele-les-secrets-de-facebook
- On ne se méfie jamais assez ...
  - http://www.zigonet.com/femme/attention-aux-jolies-espionnes-blondes-en-union-europeenne_art4106.html
- Le moteur d'Internet tourne toujours à plein régime
  - Seul problème: Apple est toujours réticent à diffuser des contenus pour iPhone
    - http://www.techcrunch.com/2009/02/11/western-europe-stimulates-worldwide-growth-in-mobile-porn/

Fun

- Le WIPS, un système pour le FUD
  - http://timesofindia.indiatimes.com/Kanpur/IIT-Kanpur-develops-anti-hacking-system/articleshow/4176482.cms
- "Les réseaux sociaux provoquent démences et cancers"
  - http://www.medialifemagazine.com/artman2/publish/New_media_23/Stunner_Social_networks_may_sicken_us.asp

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 7 avril 2009
- JSSI 2009 le 17 mars 2009
  - http://www.ossir.org/jssi/
- N'hésitez pas à proposer des sujets et des salles