OSSIR
Groupe Paris

Réunion du 11 mai 2010

Revue des dernières vulnérabilités

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

Avis Microsoft (1/10)

- **Correctifs d'Avril 2009**
  - **11 bulletins, 25 failles**
  - **Avec [exploitability index]**
  - **MS10-019 Faille(s) dans la vérification de signature [2,2]**
    - **Affecte: Windows (toutes versions supportées)**
    - **Exploit:**
      - **un EXE ou un CAB signé peut être modifié tout en conservant une signature Authenticode "valide"**
      - **l'attaque permet d'utiliser des signatures Authenticode v1 au lieu de v2 ... il reste à contourner Authenticode v1 !**
    - **Crédit: n/d**

Avis Microsoft (2/10)

- MS10-020 Faille(s) dans le client SMB [3,3,2,2,3]
  - Affecte: Windows (toutes versions supportées)
  - Exploit:
    - déni de service
    - exécution de code à distance sans authentification
      - http://g-laurent.blogspot.com/2010/04/ms10-020.html
      - http://archives.neohapsis.com/archives/fulldisclosure/2010-04/0204.html
      - http://blogs.technet.com/srd/archive/2010/04/12/smb-client-update-blog-post.aspx
    - attention aux bogues "client"
      - http://g-laurent.blogspot.com/2010/04/turning-smb-client-bug-to-server-side.html
  - Crédit:
    - Mark Rabinovich / Visuality Systems
    - Laurent Gaffié / stratsec (x3) – et Renaud Feil (non crédité)

Avis Microsoft (3/10)

- **MS10-021 Elévation de privilèges dans le noyau Windows [?,?,1,1,?,?,?,?]**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit:**
    - **élévation de privilèges à l'aide d'une clé de base de registre de type REG_LINK (x5)**
      - **note: déni de service seulement à partir de Vista SP1 / Windows 2008**
    - **élévation de privilèges lors du traitement d'une exception**
    - **déni de service à l'affichage d'une image (!)**
  - **Crédit:**
    - **Matthew 'j00ru' Jurczyk & Gynvael Coldwind / Hispasec (x5)**
      - **http://gynvael.coldwind.pl/?id=298**
      - **http://j00ru.vexillium.org/?p=307&lang=en**
    - **Tavis Ormandy / Google (x2)**
    - **Martin Tofall / Obsidium Software**
  - **Références:**
      - **http://blogs.technet.com/srd/archive/2010/04/12/registry-vulnerabilities-addressed-by-ms10-021.aspx**
      - **Note: le patch détecte si le noyau a été modifié par un *rootkit* ☺**

Avis Microsoft (4/10)

- MS10-022 Faille(s) VBScript [1]
  - Affecte: Windows 2000 / XP / 2003
  - Exploit: corrige Q981169 (dite la faille "F1")
  - Crédit: n/d (faille publiée sur Full-Disclosure)

- MS10-023 Faille(s) dans Publisher [1]
  - Affecte: Publisher (toutes versions supportées)
  - Exploit: exécution de code à l'ouverture d'un fichier ".pub"
    - ZDI-10-069
  - Crédit: Lionel d'Hauenens / ZDI

Avis Microsoft (5/10)

- MS10-024 Faille(s) Exchange et SMTP [3,?]
  - Affecte:
    - Windows (toutes versions supportées incluant le composant SMTP)
    - Exchange 2000 et 2003
  - Exploit:
    - déni de service à l'aide d'une réponse DNS "MX" malformée
    - fuite d'information à l'aide de la commande STARTTLS
  - Crédit: n/d
  - Note: la société Core a découvert d'autres failles corrigées "discrètement" par le même bulletin
    - http://www.coresecurity.com/content/CORE-2010-0424-windows-smtp-dns-query-id-bugs

Avis Microsoft (6/10)

- MS10-025 Faille(s) dans Windows Media Services [1]
  - Affecte: Windows Media Services sur Windows 2000
  - Exploit:
    - exécution de code à distance à travers le port TCP ou UDP 1755
    - disponible en quelques heures dans le produit CANVAS
      - http://twitter.com/daveaitel/status/12116967544
  - Crédit: Fabien Perigaud / LEXSI
  - Références:
    - https://www.lexsi.com/abonnes/labs/adviso-cve-2010-0478.txt
    - http://cert.lexsi.com/weblog/index.php/2010/04/14/370-vulnerabilite-dans-windows-media-services
  - Petit problème: le *patch* d'origine ne corrige pas la faille !
    - http://blogs.technet.com/msrc/archive/2010/04/21/ms10-025-security-update-to-be-re-released.aspx
    - http://blogs.technet.com/msrc/archive/2010/04/23/update-on-ms10-025.aspx
    - http://blogs.technet.com/msrc/archive/2010/04/27/ms10-025-re-release-ready.aspx

Avis Microsoft (7/10)

- MS10-026 Faille(s) dans le codec MP3 [1]
  - Affecte: Windows (toutes versions supportées
    - sauf Seven / 2008 R2
  - Exploit: exécution de code à l'ouverture d'un ".avi" contenant des données MP3
  - Crédit: Yamata Li / Palo Alto Networks

- MS10-027 Faille(s) dans Windows Media Player [1]
  - Affecte: contrôle ActiveX livré avec WMP 9
  - Exploit: exécution de code à l'ouverture d'une page Web
    - ZDI-10-070
  - Crédit: anonymous / ZDI

Avis Microsoft (8/10)

- MS10-028 Faille(s) dans Visio [1,2]
  - Affecte: Visio (toutes versions supportées sauf Viewer)
  - Exploit: exécution de code à l'ouverture d'un fichier ".vsd"
    - http://archives.neohapsis.com/archives/fulldisclosure/2010-04/0185.html
  - Crédit: Bing Liu / Fortinet (x2)
  - Note: la société Core a découvert d'autres failles corrigées "discrètement" par le même bulletin
    - http://www.coresecurity.com/content/ms-visio-dxf-buffer-overflow

- MS10-029 Faille(s) ISATAP [?]
  - Affecte: Windows (toutes versions supportées)
    - sauf Seven / 2008 R2
    - et sauf Windows 2000, qui ne supporte pas ISATAP
  - Exploit: *spoofing* d'adresse source IPv6
  - Crédit: Gabi Nakibly / National EW Research & Simulation Center

Avis Microsoft (9/10)

- **Prévisions pour Mai 2010**
  - **1 bulletin critique pour Windows**
  - **1 bulletin critique pour Office**

- **Advisories**

  - **Q973811 *Extended Protection for Authentication***
    - **V1.4: mise à jour de la FAQ**

  - **Q977544 Déni de service sur SMB**
    - **V2.0: corrigé par MS10-020**

  - **Q981169 Faille(s) dans win32hlp**
    - **V2.0: corrigé par MS10-022**

  - **Q983438 *Cross-site scripting* dans SharePoint 3.0 / 2007**
    - **http://www.htbridge.ch/advisory/xss_in_microsoft_sharepoint_server_2007.html**
    - **http://blogs.technet.com/msrc/archive/2010/04/29/security-advisory-983438-released.aspx**
    - **http://blogs.technet.com/srd/archive/2010/04/29/sharepoint-xss-issue.aspx**

Avis Microsoft (10/10)

- Révisions
  - MS10-016
    - V2.0: sortie d'un correctif pour Producer 2003
  - MS10-019
    - V1.2: documentation de problèmes connus, mise à jour de la FAQ
  - MS10-024
    - V1.2: mise à jour de la FAQ

Infos Microsoft

- Sorties logicielles
  - SQL Server 2008 "R2"
    - http://www.microsoft.com/sqlserver/tour/en/default.aspx
- Autre
  - Microsoft Security Intelligence Report (SIR), volume 8
    - Juillet – Décembre 2009
      - http://www.lemagit.fr/article/microsoft-securite-france-rustines/6269/1/special-securite-microsoft-sir-2009-peu-moins-trous-autant-attaques/
  - OpenZDK pour développer des applications Zune HD
    - Il s'agit d'un SDK "non officiel" ...
      - http://www.engadget.com/2010/04/16/zune-hd-hacked-openzdk-now-available-to-developers/

Infos Réseau

- (Principales) faille(s)
  - JBoss: contournement de l'authentification sur la console d'administration
    - Il suffit de remplacer GET/POST par HEAD (!)
      - http://blog.mindedsecurity.com/2010/04/good-bye-critical-jboss-0day.html

Infos Réseau

- **Autres infos**
  - **Sortie de l'OWASP "Top Ten" version 2010**
    - **http://www.owasp.org/index.php/Top10**
  - **"Cisco Secure Development Lifecycle"**
    - **http://blogs.cisco.com/security/comments/the_cisco_secure_development_lifecycle_an_overview/**
  - **Sortie de SNORT 2.8.6**
    - **Apporte quelques nouveautés intéressantes**
      - **Recherche de n° CB**
      - **Analyse plus fine des flux HTTP (ex. compressés)**
      - **Etc.**
    - **Attention: il y a eu du changement sur le site de mise à jour des règles**
      - **Action de l'administrateur requise**

Infos Réseau

- DNSSEC sur les serveurs DNS racine: ça s'approche
  - Une "vraie fausse" racine est actuellement en test public
    - http://www.isc.org/community/blog/201002/signed-root-coming-and-what-means-you
- Ouverture des TLDs "non latin"
    - http://www.icann.org/en/announcements/announcement-05may10-en.htm

Infos Unix

- (Principales) failles
  - Le mois de la sécurité PHP
    - Organisé par Stefan Esser
    - A noter quelques failles intéressantes
      - http://www.php-security.org/2010/05/03/mops-2010-006-php-addcslashes-interruption-information-leak-vulnerability/index.html
      - http://www.php-security.org/2010/05/04/mops-2010-008-php-chunk_split-interruption-information-leak-vulnerability/index.html
  - Une faille ptrace() dans Linux
    - Sur architecture IA-64 uniquement ...
      - https://www.lwn.net/Vulnerabilities/386339/

Infos Unix

- **Autre**
  - **Ubuntu "Lucid Lynx"**
    - **La nouvelle version "LTS" d'Ubuntu**
  - **Debian propose désormais le *rollback* des paquets**
    - **http://snapshot.debian.org/**
  - **Du côté de ClamAV**
    - **Fin de support pour ClamAV < 0.95**
      - **http://www.clamav.net/lang/fr/2009/10/05/eol-clamav-094/**
      - **Les signatures pour la version 0.95 sont incompatibles avec les versions antérieures**
    - **SourceFire a désactivé à distance toutes les versions antérieures à 0.95 à travers une mise à jour des signatures (!)**
      - **http://it.slashdot.org/story/10/04/16/1646244/ClamAV-Forced-Upgrade-Breaks-Email-Servers**
    - **Par ailleurs, une signature incorrecte a provoqué le plantage de tous les ClamAV antérieurs à la version 0.96**
      - **http://lurker.clamav.net/attach/1@20100507.110656.573e90d7.attach**
  - **Mandriva est à vendre**
    - **http://www.mandrivalinux-online.org/news/news-0-87+mandriva-est-a-vendre.php**

Failles

- **Principales applications**
  - **Correctifs dans les produits Oracle pour ce trimestre**
    - **47 failles corrigées**
      - **http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2010.html**
  - **1.6.10 <= Java < 1.6.20**
    - **Corrige la faille "Java Web Start" (ainsi que d'autres !)**
      - **... publiée par Tavis Ormandy**
      - **... mais connue par au moins 3 autres personnes**
    - **Références**
      - **http://blogs.oracle.com/security/2010/04/security_alert_for_cve-2010-08.html**
      - **http://www.oracle.com/technology/deploy/security/alerts/alert-cve-2010-0886.html**

Failles

- Adobe Reader < 9.3.2, < 8.2.2
  - 15 failles corrigées
    - http://www.adobe.com/support/security/bulletins/apsb10-09.html
  - Crédits:
    - Aki Helin / Oulu University Secure Programming Group
    - Microsoft Vulnerability Research Program (MSVR) (x3)
    - Bing Liu / Fortinet
    - Haifei Li / Fortinet
      - http://archives.neohapsis.com/archives/fulldisclosure/2010-04/0186.html
    - Anonymous / ZDI
      - ZDI-10-071
    - TELUS Security Labs
      - http://archives.neohapsis.com/archives/fulldisclosure/2010-04/0203.html
    - James Quirk / Los Alamos
    - Nicolas Joly / VUPEN (x4)
    - Felipe Andres Manzano / iSIGHT Partners Global Vulnerability Partnership
    - Greg MacManus / iSIGHT Partners Labs

Failles

- Opera < 10.53
  - http://www.opera.com/support/kb/view/953/
- Google Chrome < 4.1.249.1064
  - http://googlechromereleases.blogspot.com/2010/04/stable-update-bug-and-security-fixes.html
  - (Version 4.1.249.1059)
    - http://googlechromereleases.blogspot.com/2010/04/stable-update-security-fixes.html
- La faille Pwn2Own 2010 contre Safari corrigée
  - ZDI-10-076
  - http://support.apple.com/kb/HT4131

Failles

- **Wireshark < 1.2.8**
  - **Déni de service dans le *parser* DOCSIS**
- **VLC < 1.0.6**
  - **http://www.videolan.org/security/sa1003.html**
- **Cisco Secure Desktop < 3.5.841**
  - **Faille dans le contrôle ActiveX: téléchargement et exécution de fichiers ".EXE" ...**
    - **ZDI-10-072**
    - **http://www.cisco.com/en/US/products/products_security_advisory0918 6a0080b25d01.shtml**

Failles 2.0

- **Un bogue incroyable découvert "par hasard" sur Twitter**
  - **Il est possible d'envoyer des commandes au *backend* via des twits !**
    - **http://gizmodo.com/5535536/the-real-story-behind-twitters-ridiculous-follow-bug**
    - **http://status.twitter.com/post/587210796/follow-bug-discovered-remedied**

- **Les problèmes Facebook du mois**
  - **Fuite de l'adresse IP d'un utilisateur *via* les emails de notification**
    - **http://www.binint.com/2010/05/facebook-leaks-ip-addresses.html**
  - **Consultation des clavardages de ses amis**
    - **http://eu.techcrunch.com/2010/05/05/video-major-facebook-security-hole-lets-you-view-your-friends-live-chats/**

- **Blippy: le réseau social des consommateurs**
  - **... et accessoirement des numéros de carte bleue**
    - **http://venturebeat.com/2010/04/23/blippy-credit-card-citibank/**

- **Network Solutions + faille de configuration Wordpress == *mass 0wnage* ...**
    - **http://isc.sans.org/diary.html?storyid=8647**

Malwares et spam

- Enorme FAIL de McAfee
  - La mise à jour 5958 supprime SVCHOST.EXE sur Windows XP SP3
    - http://isc.sans.org/diary.html?storyid=8656
  - McAfee fait amende honorable
    - http://mcafee.com/us/about/false_positive_response_bus.html

- *Tous* les produits de sécurité vulnérables à une *race condition* permettant de les contourner localement
  - Nom de code: KHOBE
    - http://www.matousec.com/info/articles/khobe-8.0-earthquake-for-windows-desktop-security-software.php

- Le concours PWN2KILL en marge de la conférence iAWACS 2010
    - http://www.esiea-recherche.eu/iawacs_2010.html

- Un *call center* dédié à frauder les confirmations téléphoniques
    - http://www.wired.com/threatlevel/2010/04/callservicebiz/

Actualité (francophone)

- L'examen de la loi LOPPSI 2 reporté
  - http://info.france2.fr/france/loppsi-2-et-procedure-penale-examen-reporte-62906354.html
- La CNIL est sur Facebook ☺
  - Et produit du contenu intéressant (en exclusivité !)
    - http://www.facebook.com/CNIL
- Vague de *typosquatting* contre des sites ".fr"
  - http://www.lesechos.fr/info/comm/020478193260-le-cybersquatting-frappe-de-nouveau.htm
- La NeufBox 4 (presque) Open Source
  - Des composants tiers ne peuvent pas être publiés
    - Ex. *firmware* Broadcom
  - La peur de la FSF ?
    - http://www.neufbox4.org/blog/archive/207-sources-firmware-215-sfr-neufbox

Actualité (francophone)

- **FDN attaque HADOPI devant le Conseil d'Etat**
  - **Pour vice de forme: l'ARCEP n'a pas été consultée**

- **HADOPI, suite**
  - **"*La rédaction des spécifications fonctionnelles pour la labellisation des outils de sécurisation a été confiée à Michel Riguidel, enseignant-chercheur, à Telecom Paris Tech.*"**
    - **http://www.pcinpact.com/actu/news/56726-dpi-deep-packet-inspection-hadopi.htm**

Actualité (anglo-saxonne)

- Un "incident informatique" écroule le Dow Jones
  - http://isc.sans.org/diary.html?storyid=8761
- HP rachète Palm
  - Et prévoit de développer webOS
- Symantec rachète PGP (et GuardianEdge)

Actualité (européenne)

- Le site "Information Assurance" du Conseil de l'Europe
  - Avec une liste de produits crypto "approuvés"
    - http://www.consilium.europa.eu/showPage.aspx?id=1891&lang=en

- Conférence Black Hat Europe 2010
  - http://www.blackhat.com/html/bh-eu-10/bh-eu-10-briefings.html
    - Eric Filiol vs. chiffrement Office
      - http://blogs.msdn.com/david_leblanc/archive/2010/04/16/don-t-use-office-rc4-encryption-really-just-don-t-do-it.aspx
    - Le filtre anti-XSS dans IE8 provoque ... un XSS !
      - http://blogs.technet.com/msrc/archive/2010/04/19/guidance-on-internet-explorer-xss-filter.aspx
    - FireShark: un plugin pour aller explorer le Web malveillant
      - http://www.fireshark.org/
    - Un aperçu intéressant du côté obscur
      - https://media.blackhat.com/bh-eu-10/presentations/Dereszowski/BlackHat-EU-2010-Dereszowski-Targeted-Attacks-slides.pdf

Actualité (Google)

- Chrome 5 intègre (et met à jour) nativement Flash Player
  - http://www.accessoweb.com/Google-Chrome-5-Beta-est-encore-plus-rapide_a6429.html
- Google publie une application d'entrainement à la sécurité Web
  - http://jarlsberg.appspot.com/
- Google alimente sa base de MAC/SSID WiFi
  - D'autres l'on déjà fait ... mais ça choque les allemands ☺
    - http://www.theregister.co.uk/2010/04/22/google_streetview_logs_wlans/
- Google Cloud Print
  - Ou comment résoudre le problème de l'impression depuis un téléphone ...
    - http://code.google.com/intl/fr/apis/cloudprint/

Actualité (Google)

- L'attaque "Aurora" s'intéressait (entre autres) au code source du SSO "Gaia"
  - http://www.nytimes.com/2010/04/20/technology/20google.html
- Le décompte des requêtes judiciaires reçues pour le 2ème semestre 2009
  - Classement par pays
    - http://www.google.com/governmentrequests/

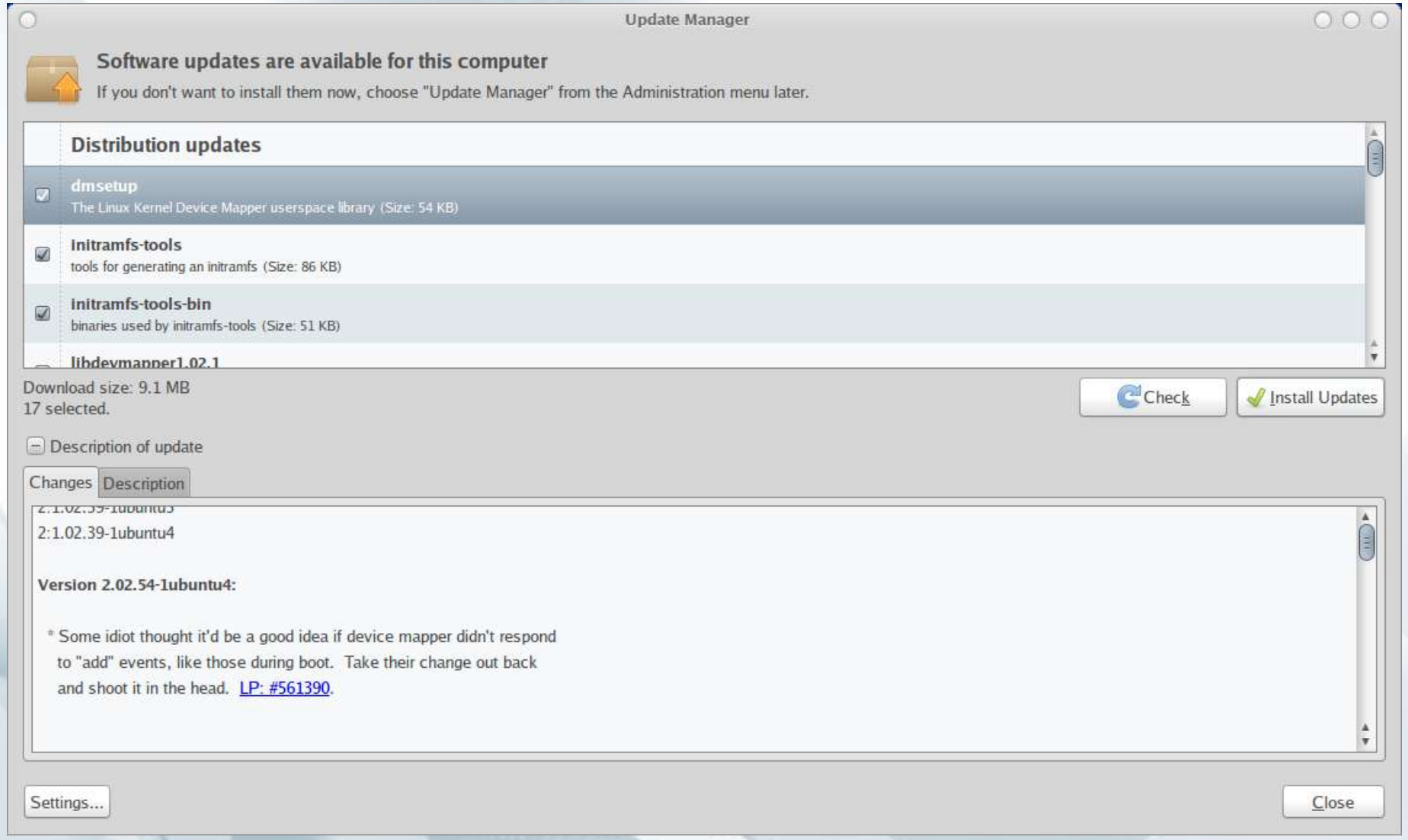
Actualité

- La GUI de Metasploit devient payante
  - http://www.metasploit.com/express/
- OpenDLP
  - Du DLP "light" ... en Open Source
    - http://code.google.com/p/opendlp/
- Sophos racheté par Apax Partners

Fun

- **Marc Maiffret: "Windows est plus sûr que Mac OS X"**
  - **http://www.neowin.net/news/hacker-says-windows-is-more-secure-than-mac-calls-apple-fans-quotignorantquot**
- **Le pirate modifie ses notes en piratant l'application Web**
  - **Problème: il a 9 ans ...**
    - **http://www.washingtonpost.com/wp-dyn/content/article/2010/04/14/AR2010041404159.html**

Fun


Update Manager
Software updates are available for this computer
If you don't want to install them now, choose "Update Manager" from the Administration menu later.
Distribution updates
dmsetup
The Linux Kernel Device Mapper userspace library (Size: 54 KB)
initramfs-tools
tools for generating an initramfs (Size: 86 KB)
initramfs-tools-bin
binaries used by initramfs-tools (Size: 51 KB)
libdevmapper1.02.1
Download size: 9.1 MB
17 selected.
Check
Install Updates
Description of update
Changes
Description
2:1.02.39-1ubuntu4
Version 2.02.54-1ubuntu4:
* Some idiot thought it'd be a good idea if device mapper didn't respond to "add" events, like those during boot. Take their change out back and shoot it in the head. LP: #561390.
Settings...
Close

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 8 juin 2010
- N'hésitez pas à proposer des sujets et des salles