OSSIR
Groupe Paris

Réunion du 11 octobre 2011

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Septembre 2011**
  - **5 bulletins, 15 failles**
  - **MS11-070 Faille dans WINS**
    - **Affecte: Windows 2003 / 2008 / 2008R2**
      - **Sauf certains systèmes Itanium**
    - **Exploit: élévation de privilèges locale**
      - **http://www.coresecurity.com/content/ms-wins-ecommenddlg-input-validation**
    - **Crédit: Nicolas Economou / Core Security Technologies**

Avis Microsoft

- **MS11-071 *DLL Preloading***
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit: fichiers ".rtf", ".txt" et ".doc"**
  - **Crédit: n/d**

- **MS11-072 Failles dans Excel (x6?)**
  - **Affecte: Excel (toutes versions supportées)**
    - **Y compris Viewer, SharePoint, Web Apps, Mac OS X …**
  - **Exploit: exécution de code à l'ouverture d'un fichier malformé**
  - **Crédit:**
    - **Anonymous / iDefense**
    - **Sean Larsson / iDefense Labs**
    - **Anonymous / iDefense**
    - **Anonymous / ZDI**
    - **Omair / ZDI**

Avis Microsoft

- **MS11-073 Failles dans Office (x2)**
  - **Affecte: Office 2003, 2007, 2010**
  - **Exploit:**
    - **Exécution de code à l'ouverture d'un fichier Office malformé**
    - ***DLL Preloading***
  - **Crédit:**
    - **Parvez Anwar / Secunia Research**
    - **David Warren / CERT/CC**

- **MS11-074 Failles dans SharePoint (x6)**
  - **Affecte: Groove, SharePoint, Forms, Web Apps**
    - **Sauf SharePoint 2003 SP3**
  - **Exploit:**
    - **XSS**
    - **Lecture de fichiers arbitraires sur le serveur (via XML)**

Avis Microsoft

- Exploit (suite):
  - http://www.seekersec.com/Advisories/SeekerAdvMS03.html
  - http://www.seekersec.com/Advisories/SeekerAdvMS04.html
- Crédit:
  - Andrew Connell / Critical Path Training, LLC
  - David Feldman / Raytheon
  - Adi Cohen / IBM Rational Application Security
  - Trend Micro
  - Pedro Jimenez / ITT
  - "Seeker automatic application security testing solution"
  - Nicolas Grégoire / Agarri
  - Jim LaValley / LaValley Consulting, LLC
  - Irene Abezgauz / Seeker

Avis Microsoft

- **Advisories**
  - **Q2269637 *DLL Preloading***
    - **V10.0: publication des bulletins MS11-071 et MS11-073**
  - **Q2588513**
    - **V1.0: publication de l'attaque B.E.A.S.T.**
  - **Q2607712 Révocation du certificat DigiNotar**
    - **V4.1: disponibilité d'un correctif (Q2616676) pour Windows Developer Preview**
    - **V5.0: re-publication complète du bulletin**

Avis Microsoft

- Révisions
  - MS10-035
    - V2.0: problème de détection sur Windows 2000 et Windows XP
  - MS11-043
    - V2.1: correction d'une clé de base de registre
  - MS11-049
    - V2.1: changement dans la logique de détection
  - MS11-058
    - V1.1: MS11-046 n'est pas remplacé par ce correctif
  - MS11-074
    - V1.1: ajout d'un lien manquant
    - V1.2: suppression d'un lien erroné

Infos Microsoft

- **Sorties logicielles**
  - **Windows Phone "Mango"**
  - **Visual Studio 11, .NET 4.5 (Preview)**
  - **Windows 8 (Preview)**
    - **Un antivirus natif**
      - **http://www.linformaticien.com/actualites/id/21600/windows-8-integrera-un-antivirus-en-natif.aspx**
    - **Pas de Flash en mode "tablette"**
      - **http://www.linformaticien.com/actualites/id/21599/microsoft-bannit-flash-des-tablettes-windows-8.aspx**
    - **Réécriture dynamique des sections de code**
      - **Anti-ROP**

Infos Microsoft

- Autre
  - Microsoft démantèle le botnet Kelihos
    - http://blogs.technet.com/b/mmpc/archive/2011/09/26/operation-b79-kelihos-and-additional-msrt-september-release.aspx
  - MS11-035: les détails
    - http://seclists.org/bugtraq/2011/Sep/77
  - L'accident bête
    - Microsoft Security Essentials détecte Chrome comme un virus ☺
      - http://chrome.blogspot.com/2011/09/problems-with-microsoft-security.html
  - La Russie pourrait financer le projet ReactOS
    - http://www.linformaticien.com/actualites/id/21616/la-russie-pourrait-financer-un-clone-de-windows.aspx

Infos Réseau

- (Principales) faille(s)
  - Les failles Cisco
    - 10 bulletins dans la vague principale
      - http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep11.html
    - Plus quelques autres
      - http://www.cisco.com/warp/public/707/cisco-sa-20110914-cusm.shtml
      - http://www.cisco.com/warp/public/707/cisco-sa-20110914-lms.shtml
      - http://www.cisco.com/warp/public/707/cisco-sa-20110920-ise.shtml
      - http://www.cisco.com/warp/public/707/cisco-sa-20111005-fwsm.shtml
      - http://www.cisco.com/warp/public/707/cisco-sa-20111005-asa.shtml
      - http://www.cisco.com/warp/public/707/cisco-sa-20111005-nac.shtml

Infos Réseau

@41414141
FX of Phenoelit

Congratulations Cisco! Remotely crashing MPLS cloud routers with valid ICMPv6 packets. A new all-time-record-fail!
cisco.com/warp/public/70...

29 Sep via web ☆ Favori ↻ Retweeter ↩ Répondre

Retweeté par approximatehack et 92 autres

Infos Unix

- **(Principales) faille(s)**
  - **Apache Tomcat #epic #fail**
    - **Sur l'authentification HTTP Digest**
      - **http://permalink.gmane.org/gmane.comp.apache.maven.announce/1048**
  - **CVE-2011-3192 (DoS Apache) corrigé dans les produits Oracle**
    - **My Oracle Support Note 1357871.1**
  - **APT-KEY ne vérifie pas les signatures**
    - **Juste les KeyIDs …**
      - **http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=642480**
  - **mod_proxy**
    - **Fuite d'information avec certaines règles**
      - **http://seclists.org/fulldisclosure/2011/Oct/232**
  - **Yubikey: le mot de passe vide marche aussi ☺**
      - **https://github.com/Yubico/yubico-pam/commit/4712da70cac159d5ca9579c1e4fac0645b674043**

Infos Unix

- **Autre**
  - **Kernel.org intégralement reconstruit**
    - **https://lwn.net/Articles/460376/**

Failles

- Principales applications
  - Adobe Reader < 10.1.1
    - 13 failles corrigées
      - http://www.adobe.com/support/security/bulletins/apsb11-24.html
    - Dont une évasion de la sandbox
      - http://www.fortiguard.com/advisory/FGA-2011-30.html
    - Crédit
      - Paul Sabanal & Mark Yason / IBM X-Force
      - Zhenhua Liu / Fortinet
      - Vladimir Vorontsov / ONsec
      - binaryproof / ZDI (x8)
      - James Quirk / Los Alamos
      - Anonymous / iDefense
      - Tavis Ormandy / Google
      - Hossein Lotfi / Secunia
  - Adobe Flash Player < 11.0.1.152
    - Pas un correctif de sécurité ?
  - Adobe Flash Player < 10.3.183.10
    - http://www.adobe.com/support/security/bulletins/apsb11-26.html
  - Adobe Photoshop Elements
    - http://www.adobe.com/support/security/advisories/apsa11-03.html

Failles

- Google Chrome < 14.0.835.202
- Google Chrome < 14.0.835.163
  - http://googlechromereleases.blogspot.com/2011/09/stable-channel-update_16.html
- FireFox < 3.6.23
  - http://www.mozilla.org/security/known-vulnerabilities/firefox36.html#firefox3.6.23
- ThunderBird < 7
  - http://www.mozilla.org/security/known-vulnerabilities/thunderbird.html#thunderbird7
- FireFox < 7
  - http://www.mozilla.org/security/known-vulnerabilities/firefox.html#firefox7
- VMWare WorkStation < 7.1.5
  - VMSA-2011-0011

Failles 2.0

- Enorme faille dans une application HTC
  - Permet à n'importe quelle autre application d'accéder aux messages, etc.
    - http://arstechnica.com/gadgets/news/2011/10/security-hole-in-htc-phones-gives-up-e-mail-addresses-location.ars
- Facebook continue à traquer les utilisateurs après *logout*
    - http://nikcub.appspot.com/logging-out-of-facebook-is-not-enough
- Comment nuire à Facebook ?
  - Exiger toutes ses données sur un CD-ROM ☺
    - http://www.presse-citron.net/comment-embeter-facebook-tres-simplement
- 25% des extensions Chrome sont mal foutues
    - http://www.net-security.org/secworld.php?id=11709
- Un guide de développement "sécurisé" pour applications Web
    - https://wiki.mozilla.org/WebAppSec/Secure_Coding_Guidelines

Sites piratés

- Les sites piratés du mois
  - Areva """"renforce sa sécurité""""
    - http://www.cnis-mag.com/hack-areva-analyse-%E2%80%A6a-chaud.html
    - http://lexpansion.lexpress.fr/entreprise/areva-victime-d-une-attaque-informatique-de-grande-ampleur_263462.html
  - 4,9 millions de dossiers médicaux au Texas
    - Volés dans la voiture d'un sous-traitant
      - http://www.reuters.com/article/2011/09/29/us-data-breach-texas-idUSTRE78S5JG20110929
  - 20 000 dossiers médicaux en ligne … depuis 1 an
    - http://www.nytimes.com/2011/09/09/us/09breach.html?_r=2
  - Mitsubishi Heavy Industries Ltd
    - La division militaire de Mitsubishi
      - http://www.reuters.com/article/2011/09/19/us-mitsubishiheavy-computer-idUSTRE78I0EL20110919

Sites piratés

- MySQL.com
  - http://blog.armorize.com/2011/09/mysqlcom-hacked-infecting-visitors-with.html
- OTAN
  - http://www.otan.us/timac/timacdata/index.cfm?fuseaction=userPasswords
- American Express
  - http://qnrq.se/full-disclosure-american-express/
- Une liste à la Prévert
  - http://pastebin.com/LaKrWgXT
- Note: DigiNotar a fermé
  - http://www.vasco.com/company/press_room/news_archive/2011/news_vasco_announces_bankruptcy_filing_by_diginotar_bv.aspx

Malwares et spam

- Mebromi
  - Un virus s'implante dans les BIOS "Award"
    - http://blog.webroot.com/2011/09/13/mebromi-the-first-bios-rootkit-in-the-wild/
- McAfee "DeepSAFE"
  - Un antivirus dans l'hyperviseur …
    - http://www.mcafee.com/us/solutions/mcafee-deepsafe.aspx

Actualité (francophone)

- Keynectis fusionne avec OpenTrust
  - http://www.securityvibes.fr/marche-business/keynectis-opentrust/
- Un projet d'antivirus "made in France"
  - http://www.lesechos.fr/innovation/technologies/0201657345459-un-projet-d-antivirus-made-in-france-224686.php
- Le NFC mobile revient en France
  - http://www.clubic.com/telephone-portable/operateur-telephonie-mobile/orange/actualite-447738-samsung-galaxy-ii-nfc-orange.html
- La dernière mise à jour Livebox réinitialise le mot de passe "admin" à … "admin"
  - http://korben.info/mot-de-passe-livebox.html

Actualité (européenne)

- La notification des incidents de sécurité bientôt obligatoire partout et pour tous ?
  - http://www.scmagazineuk.com/exclusive-european-businesses-face-mandatory-disclosure-law/article/212988/
- Les effets secondaires du Patriot Act
  - Les Pays-Bas envisagent d'exclure les sociétés américaines des marchés publics de Cloud
    - http://www.lemagit.fr/article/etats-unis-europe-cloud-computing-legislation/9479/1/cloud-patriot-act-les-pays-bas-reflechissent-exclure-les-americains-des-contrats-gouvernementaux/

Actualité (Google)

- Google Flights
  - https://www.google.com/flights/

Actualité (Apple)

- **Mac OS X Lion #epic #fail**
  - **Il est possible d'énumérer et de changer le mot de passe de n'importe quel utilisateur**
    - **http://www.defenceindepth.net/2011/09/cracking-os-x-lion-passwords.html**

- **Steve Jobs R.I.P.**
  - **http://www.apple.com/stevejobs/**

Actualité (crypto)

- L'attaque B.E.A.S.T.
  - Implémentation d'une attaque connue sur TLS <= 1.0
    - http://threatpost.com/en_us/blogs/new-attack-breaks-confidentiality-model-ssl-allows-theft-encrypted-cookies-091611
  - Quelques conditions de mise en œuvre …
    - Attaque à clair connu
  - *Workaround*: utiliser un chiffrement par flot plutôt que par bloc

Actualité

- **Conférences**
  - **Assises de la Sécurité 2011**
    - **La conférence de clôture de Patrick Pailloux**
      - **http://www.zdnet.fr/actualites/patrick-pailloux-anssi-les-si-en-france-sont-aujourd-hui-en-danger-39764675.htm**
    - **Le troll**
      - **https://twitter.com/#!/pentesteur/status/121890646947676160/photo/1**
  - **Appel à communications pour SSTIC 2012**
    - **http://www.sstic.org/2012/news/**

Actualité

- **Sorties logicielles**
  - **VMWare WorkStation 8.0**

Actualité

- **Le CCC ciblé par un cheval de Troie**
  - **Celui de la police allemande ?**
    - **http://www.f-secure.com/weblog/archives/00002249.html**

- **Samsung + Intel (MeeGo) = Tizen**
  - **Quid de BadaOS, etc. ?**
    - **http://www.linformaticien.com/actualites/id/21717/samsung-et-intel-developpent-tizen-un-os-mobile-open-source.aspx**

Fun

- **Hacker High School**
  - **http://spectrum.ieee.org/at-work/education/hacker-high-school**
- **Nouvelle règle chez Sony**
  - **Vous ne pouvez pas leur faire de procès si vous êtes client ☺**
    - **http://blog.eset.com/2011/09/15/sony-new-terms-of-service-you-can%E2%80%99t-file-a-class-action-suit**
- **Firmware LOL**
  - **https://admin.fedoraproject.org/updates/F14/FEDORA-2011-12302**

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 8 novembre 2011
- N'hésitez pas à proposer des sujets
- L'appel à communications pour la JSSI 2012 est sorti
  - Thème: *L'intrusion, outil essentiel de la SSI ?*
  - Deadline pour les soumissions: 5 décembre 2011