# OSSIR
# Groupe Paris

## Réunion du 8 novembre 2011

# Revue des dernières vulnérabilités

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

# Avis Microsoft

- **Octobre 2011**
  - **8 bulletins, XXX failles**
  - **MS11-075 DLL Preloading dans "Active Accessibility" [1]**
    - **Affecte: Windows (toutes versions supportées)**
    - **Exploit: DLL Preloading**
    - **Crédit:**
      - **Mila Parkour / contagiodump**
      - **Anshul Kothari & Nishant Kaushik / Adobe**

# Avis Microsoft

- MS11-076 DLL Preloading dans "Media Center" [1]
  - Affecte:
    - Windows Vista, Windows 7
    - Media Center TV Pack for Windows Vista
  - Exploit: DLL Preloading
  - Crédit: n/d

- MS11-077 Failles dans des pilotes Windows (x4) [1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: élévation de privilèges à l'ouverture d'un fichier de polices
    - Exemple: fichier ".FON"
  - Crédit:
    - Andrei Lutas / BitDefender
    - Tarjei Mandt / Norman
    - Maik Wellmann
    - Will Dorman / CERT/CC

# Avis Microsoft

- **MS11-078 Faille .NET [1]**
  - **Affecte:**
    - **.NET Framework (toutes versions supportées, hors 3.5SP1)**
    - **SilverLight 4**
  - **Exploit: exécution de code arbitraire depuis une *assembly* .NET**
  - **Crédit: anonymous / Beyond Security Secure Disclosure**

- **MS11-079 Failles dans ForeFront UAG (x5) [1]**
  - **Affecte: ForeFront UAG 2010 (toutes versions supportées)**
  - **Exploit:**
    - **XSS (x3)**
    - **Déni de service**
    - **Exécution de code arbitraire au travers de l'applet Java**
  - **Crédit:**
    - **Tenable Network Security (x3)**
    - **Elisabeth Demeter / SEC Consult**
      - **https://www.sec-consult.com/en/advisories.html#a72**

# Avis Microsoft

- MS11-080 Faille dans AFD.SYS [1]
  - Affecte: Windows XP / 2003 (toutes versions supportées)
  - Exploit: élévation de privilèges locale
  - Crédit: Bo Zhou / National University of Defense Technology (Chine)

- MS11-081 Correctif cumulatif pour IE (x8) [1]
  - Affecte: IE (toutes versions supportées)
  - Exploit: exécution de code
    - ZDI-11-287, ZDI-11-288, ZDI-11-289, ZDI-11-290
  - Crédit:
    - Vishwas Sharma / McAfee Labs
    - David Bloom / Greplin (x3)
    - Ivan Fratic + ZDI (x2)
      - http://ifsec.blogspot.com/2011/10/internet-explorer-select-element-remote.html
    - GWSlabs + VeriSign
    - Sebastian Apelt + ZDI
    - Anonymous + ZDI
    - Eduardo Vela Nava / Google
    - Soroush Dalili
    - Billy Rios / Google

# Avis Microsoft

- MS11-082 Faille dans Host Integration Server (x2) [n/a]
  - Affecte: HIS 2004 SP1, HIS 2006 SP1, HIS 2009, HIS 2010
    - Mais pas HIS 2000 SP2
  - Exploit: déni de service
    - Au travers des ports UDP/1478, TCP/1477, TCP/1478
  - Crédit: n/d

# Avis Microsoft

- **Prévisions pour Novembre 2011**
  - 4 bulletins affectant Windows
- **Nouvelles informations**
  - La faille Visio MS11-060 affecte également Publisher
    - http://www.coresecurity.com/content/publisher-pubconv-memory-corruption
- **Advisories**
  - Q2269637 DLL Preloading
    - V11.0: ajout des bulletins MS11-075 et MS11-076
  - Q2639658 Vulnérabilité dans le support des polices TTF
    - Elévation de privilèges locale permettant d'exécuter du code en mode noyau
    - Découvert "dans la nature" dans Win32.DuQu
    - V1.0: publication de l'avis
    - V1.2: correction du workaround

# Avis Microsoft

- Révisions
  - MS10-070
    - V4.2: ajout de la plateforme 2008 R2 x64 Server Core + .NET 4
  - MS10-077
    - V3.1: ajout de la plateforme 2008 R2 x64 Server Core + .NET 4
  - MS11-028
    - V2.3: ajout de la plateforme 2008 R2 x64 Server Core + .NET 4
  - MS11-039
    - V1.1: ajout de la plateforme 2008 R2 x64 Server Core + .NET 4
  - MS11-044
    - V1.1: changement dans la logique de détection
    - V1.2: ajout de la plateforme 2008 R2 x64 Server Core + .NET 4
  - MS11-058
    - V1.2: changement dans la logique de détection
  - MS11-066
    - V1.1: ajout de la plateforme 2008 R2 x64 Server Core + .NET 4
  - MS11-069
    - V1.2: ajout de la plateforme 2008 R2 x64 Server Core + .NET 4

# Avis Microsoft

- MS11-072
  - V1.1: changement dans la logique de détection
- MS11-074
  - V1.3: changement dans la logique de détection
- MS11-075
  - V1.1: changement documentaire
  - V1.2: correction sur le nom des fichiers
- MS11-078
  - V1.1: correction sur la nécessité de redémarrage avec .NET 1.1 SP1
  - V1.2: ajout de la plateforme 2008 R2 x64 Server Core + .NET 4
- MS11-081
  - V1.1: ajout d'un problème connu
  - V1.2: correction d'un problème connu avec IE7

# Infos Microsoft

- **Sorties logicielles**
  - **SQL Server 2008 SP3**
  - **Office 2007 et SharePoint 2007 SP3**
    - **Note: fin du support *mainstream* en avril 2012**
      - **http://blogs.technet.com/b/office_sustained_engineering/archive/2011/10/06/announcing-service-pack-3-for-office-2007-and-sharepoint-server-2007.aspx**

# Infos Microsoft

- **Autre**
  - **Microsoft Security Intelligence Report (SIR), Volume 11**
    - **Avec la contribution de Mark Russinovitch**
      - **http://www.microsoft.com/sir**
  - **Windows 8 en mode "Metro" n'aura pas de plugins**
    - **Est-ce la fin de SilverLight ?**
      - **http://www.sharepoint-ch.com/welcome-windows-8-rip-silverlight-or-not?mid=521**
  - **Le compte YouTube de Microsoft piraté**
    - **http://www.numerama.com/magazine/20294-le-compte-youtube-de-microsoft-pirate.html**
  - **Microsoft touche de l'argent sur la moitié des téléphones Android vendus dans le monde ☺**
    - **http://arstechnica.com/microsoft/news/2011/10/microsoft-collects-license-fees-on-50-of-android-devices-tells-google-to-wake-up.ars**

# Infos Réseau

- (Principales) faille(s)
  - Déni de service contre SSL
    - "By design": l'établissement de connexion est 15x plus coûteux côté serveur que côté client
      - https://thehackerschoice.wordpress.com/2011/10/24/thc-ssl-dos/
  - Déni de service reposant sur les serveurs de jeu en ligne
      - http://cert.lexsi.com/weblog/index.php/2011/10/18/422-new-dos-attack-amplified-through-gaming-servers

# Infos Réseau

- **Autres infos**
  - **Une panne Juniper + BGP perturbe Internet**
    - **http://www.bortzmeyer.org/crash-internet-nov-2011.html**
  - **Empoisonnement DNS massif au Brésil**
    - **http://www.securelist.com/en/blog/208193214/Massive_DNS_poisoning_attacks_in_Brazil**
  - **Incendie chez Cogent à Rennes**
    - **http://www.mail-archive.com/frnog@frnog.org/msg16299.html**

# Infos Unix

- (Principales) faille(s)
  - FreeBSD
    - *Stack overflow* dans la fonction bind() …
      - http://permalink.gmane.org/gmane.os.freebsd.security.announce/206
  - Le cas d'école de la mauvaise application
    - Et de la mauvaise communication
      - https://bugs.launchpad.net/calibre/+bug/885027

# Infos Unix

- **Autre**
  - **Sortie (discrète) de Linux 3.1**

# Failles

- **Principales applications**
  - **Oracle Quaterly Patch**
    - **57 failles corrigées**
      - **http://www.oracle.com/technetwork/topics/security/cpuoct2011-330135.html**
      - **http://www.teamshatter.com/topics/general/team-shatter-exclusive/sql-injection-vulnerability-in-oracle-drop-index-for-spatial-datatypes/**
      - **http://www.teamshatter.com/topics/general/team-shatter-exclusive/buffer-overflow-in-oracle-database-ctxsys-drvdisp-tablefunc_asown-function/**
    - **Java < 1.6.0_29**
      - **http://www.oracle.com/technetwork/topics/security/javacpuoct2011-443431.html**
      - **http://www.oracle.com/technetwork/java/javase/6u29-relnotes-507960.html**
      - **ZDI-11-305, ZDI-11-306, ZDI-11-307**
    - **Mis en *blacklist***
      - **Cisco AnyConnect Mobility Client**
      - **Microsoft UAG Client**
  - **Oracle NoSQL**
    - **Le retour du ../../..**
      - **http://seclists.org/fulldisclosure/2011/Nov/58**

# Failles

- Apple
  - Mac OS X < 10.7.2
    - http://support.apple.com/kb/HT5002
  - iOS < 5.0
    - CalDav ne vérifie pas le certificat SSL serveur …
    - http://seclists.org/fulldisclosure/2011/Oct/544
  - iTunes < 10.5
    - http://support.apple.com/kb/HT4981
  - QuickTime < 7.7.1
    - http://support.apple.com/kb/HT5016
    - ZDI-11-295
    - ZDI-11-303, ZDI-11-304
    - ZDI-11-311, ZDI-11-312, ZDI-11-313, ZDI-11-314, ZDI-11-315, ZDI-11-316

# Failles

- Adobe Reader 10.1.1 corrigeait …
  - ZDI-11-296 … ZDI-11-302
  - ZDI-11-310
- Chrome < 15.0.874.102
  - http://googlechromereleases.blogspot.com/2011/10/chrome-stable-release.html
- Chrome < 15.0.874.106
  - N'apporte pas de correction de sécurité
  - http://googlechromereleases.blogspot.com/2011/10/stable-channel-update_26.html
- WireShark < 1.6.3
- Ruby #fail
  - Le module RSA est toujours … 1
    - https://github.com/ruby/ruby/commit/ab682d95e077b43db7dfd293744aa546888d7e35

# Failles 2.0

- Il détecte des failles énormes dans le site de l'entreprise
  - … et reçoit la facture du correctif quelques jours après
    - http://www.scmagazine.com.au/News/276678,researcher-discloses-vulnerability-to-firm-gets-police-visit.aspx
- Facebook autorisait *l'upload* de .EXE
    - http://www.securitypentest.com/2011/10/facebook-attach-exe-vulnerability.html
- A quoi servent les comptes volés ?
  - Ils ne sont pas perdus pour tout le monde …
    - http://blog.eu.playstation.com/2011/10/12/an-important-message-from-sonys-chief-information-security-officer/
  - Moralité: ne réutilisez pas vos mots de passe sur différents sites !

# Sites piratés

- Les sites piratés du mois
  - Les industries chimiques piratées "en masse"
    - Opération "Nitro"
      - http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf
  - La cyberguerre fait parfois des vrais morts
    - http://cyberwarzone.com/cyberwarfare/diginotar-death-cases-iran-diginotarhack
  - 40 sites pédophiles piratés par Anonymous
    - http://www.digitaltrends.com/web/anonymous-wages-war-on-darknet-hidden-pedophiles-40-websites-down/
  - Le visage du piratage
    - EDF, Floyd Landis … ont fait appel au même homme
      - http://www.linformaticien.com/actualites/id/21863/piratage-alain-quiros-affole-edf-floyd-landis-vivendi.aspx
  - La liste des victimes potentielles du "Hack RSA"
      - http://krebsonsecurity.com/2011/10/who-else-was-hit-by-the-rsa-attackers/
    - Note: plein de gens utilisent encore SecurID
      - https://webmail.act.nato.int/

# Malwares et spam

- Un ver JBoss
  - … exploitant une faille vieille de plusieurs années
    - http://community.jboss.org/blogs/mjc/2011/10/20/statement-regarding-security-threat-to-jboss-application-server
- 99,8% des infections en ligne liés à 5 logiciels tiers …
  - Java, Adobe Reader, Adobe Acrobat, Flash Player, QuickTime
    - http://www.theregister.co.uk/2011/09/28/window_malware_infection_exposed/
- Un nouveau ver "SCADA"
  - W32/DuQu
    - http://www.crysys.hu/
    - http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet
  - Un détecteur à base de signatures
    - https://github.com/halsten/Duqu-detectors/blob/84eafcb95f4b1cf3708803f484398245f08e582c/DuquDriverPatterns.py
- Un simple iPhone posé à côté d'un clavier peut servir de keylogger hardware
  - En mesurant les vibrations de la table
    - http://nakedsecurity.sophos.com/2011/10/20/iphone-spyware-snoop-desktop-typing/

# Actualité (francophone)

- Les outils EBIOS 2010 sont sortis
  - Ils sont en Flash ☺
    - https://adullact.net/projects/ebios2010/
- Oh, surprise
  - Le filtrage d'Internet s'étend désormais aux violations du droit de la consommation
    - http://www.numerama.com/magazine/19950-la-dgccrf-pourra-faire-bloquer-un-site-violant-le-droit-des-consommateurs.html
- La carte d'identité numérique & biométrique votée au Sénat
    - http://www.linformaticien.com/actualites/id/22077/adoption-de-la-carte-d-identite-numerique-securisee-au-senat.aspx
- Les français lisaient tous les mails de l'ambassade UK
  - Car aucun chiffrement n'était utilisé
    - http://www.v3.co.uk/v3-uk/security-watchdog-blog/2120579/sacre-bleu-french-snooped-british-government-emails

# Actualité (francophone)

- La liste des agences autorisées à pratiquer "la captation de données informatiques"
  - JORFTEXT000024752774
- L'espionnage se pratique aussi "à l'ancienne"
  - http://www.lefigaro.fr/actualite-france/2011/10/12/01016-20111012ARTFIG00436-nouvelle-affaire-d-espionnage-chinois-en-france.php
- Le site CopWatch filtré en référé
  - Par DNS et par IP
  - Chez les FAI "grand public" majeurs
  - Les FAI seront indemnisés
    - http://www.liberation.fr/societe/01012365753-copwatch-interdit-d-acces-en-france

# Actualité (anglo-saxonne)

- Les drones américains attaqués par un virus
  - http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/
  - Ou pas ..
    - http://news.techworld.com/security/3310695/malware-found-on-us-drone-base-was-gaming-keylogger/
    - http://www.myfoxny.com/dpp/news/military-computer-virus-wasnt-directed-at-drones-20111012-apx
- Le gouvernement anglais recrute des hackers
  - Lui aussi ☺
    - http://digital.cabinetoffice.gov.uk/2011/10/25/the-second-lever/
- "La Chine mobilise ses cyber-milices"
  - Réalité ou fantasme américain ?
    - http://www.ft.com/intl/cms/s/0/33dc83e4-c800-11e0-9501-00144feabdc0.html

# Actualité (européenne)

- Europe vs. Facebook
  - Le combat d'un individu
    - http://europe-v-facebook.org/EN/en.html
- Le scandale du spyware gouvernemental s'étend en Allemagne
    - http://www.dw-world.de/dw/article/0,,15475258,00.html

# Actualité (Google)

- Google abandonne certains produits
  - Dont Google Code Search ☹
    - http://googleblog.blogspot.com/2011/10/fall-sweep.html
- L'API Google Maps désormais payante
  - … pour une utilisation en volume (> 25,000 accès par jour)
    - http://www.linformaticien.com/actualites/id/22005/google-fait-desormais-payer-l-api-google-maps.aspx
- Android 4.0 disponible
    - http://www.linformaticien.com/actualites/id/21876/google-devoile-android-4-0.aspx
    - http://www.linformaticien.com/actualites/id/21879/lancement-du-samsung-galaxy-nexus-1er-smartphone-android-4-0.aspx
- Dolphin Browser sur Android est malveillant !
    - http://arstechnica.com/gadgets/news/2011/10/major-privacy-flaw-found-in-dolphin-hd-browser-for-android.ars
- Un *framework* de *pentest* sur plateforme Android
    - http://zimperium.com/anti.html

# Actualité (Google)

- Le centre de recherches parisien enfin opérationnel ?
  - Inauguration le 6 décembre
    - http://www.lexpress.fr/actualite/indiscrets/google-s-aggrandit-a-paris_1039934.html
- L'empreinte écologique (ou pas) de Google
  - Google consomme 0,01% de l'électricité mondiale
    - http://www.greenit.fr/article/acteurs/empreinte-carbone-google-a-emis-146-million-de-tonnes-de-co2-en-2010-3949
- "do a barrel roll"

# Actualité (Apple)

- Sortie de iOS 5
  - Et du fameux iCloud …
    - http://www.infoworld.com/d/mobile-technology/does-icloud-make-iphones-and-ipads-security-risk-925?page=0,0
  - … ainsi qu'un bogue épuisant la batterie

- Sortie de l'iPhone 4S
  - Et déjà des failles dans Siri ☺
    - http://www.securityvibes.fr/menaces-alertes/siri-iphone/
  - … ainsi qu'une panne de Siri (qui fonctionne en ligne)
    - http://www.linformaticien.com/actualites/id/22086/panne-de-siri-plus-d-informations.aspx

- iOS 5 est bientôt jailbreaké
  - http://www.linformaticien.com/actualites/id/22024/l-iphone-4s-sous-ios-5-est-jailbreake.aspx

# Actualité (Apple)

- **Contournement de la signature des applications iOS**
  - **Charlie Miller, Syscan**
    - **http://threatpost.com/en_us/blogs/new-ios-bug-lets-apps-run-unsigned-code-110711**
- **Le sandboxing de toutes les applications Mac OS X**
  - **Obligatoire en mars 2012 ?**
    - **http://www.macrumors.com/2011/11/02/mac-app-store-sandboxing-requirement-pushed-to-march-as-uncertainty-looms/**
- **CNIL vs. Apple**
  - **http://www.linformaticien.com/actualites/id/21827/votre-iphone-raconte-votre-vie-pendant-la-nuit.aspx**

# Actualité (crypto)

- XML-Encryption est cassé
  - Encore un "*padding oracle*" contre le mode CBC
    - http://arstechnica.com/business/news/2011/10/researchers-break-w3c-encryption-standard-for-xml.ars
  - Conséquences
    - Les solutions de Cloud Amazon EC2 et Eucalyptus étaient vulnérables
    - http://www.h-online.com/security/news/item/Researchers-find-holes-in-the-cloud-1366112.html
- Eric Filiol vs. Tor
    - http://www.itespresso.fr/securite-it-la-confiance-dans-le-reseau-d-anonymisation-tor-est-ebranlee-47287.html
    - https://lists.torproject.org/pipermail/tor-talk/2011-October/021730.html
- Perseus choisi pour protéger LibreOffice OnLine (LOOL)
    - http://twitter.com/#!/efiliol/status/114960899248369664

# Actualité

- Conférences
- Sorties logicielles
  - Cuckoo Sandbox
    - http://www.cuckoobox.org/about.php
  - Android Reverse Engineering VM
    - http://redmine.honeynet.org/projects/are/wiki

# Actualité

- BlackBerry en panne mondiale
  - Pendant plusieurs jours
    - http://fr.blackberry.com/serviceupdate/
    - http://www.linformaticien.com/actualites/id/21818/rim-confirme-la-panne-mondiale-et-la-repare-en-20-heures.aspx
- Bouygues Telecom également en panne
    - http://www.linformaticien.com/actualites/id/21874/apres-rim-le-reseau-bouygues-telecom-s-effondre.aspx
- WikiLeaks
  - … n'a plus d'argent
  - … et Julian Assange a été extradé vers la Suède

# Actualité

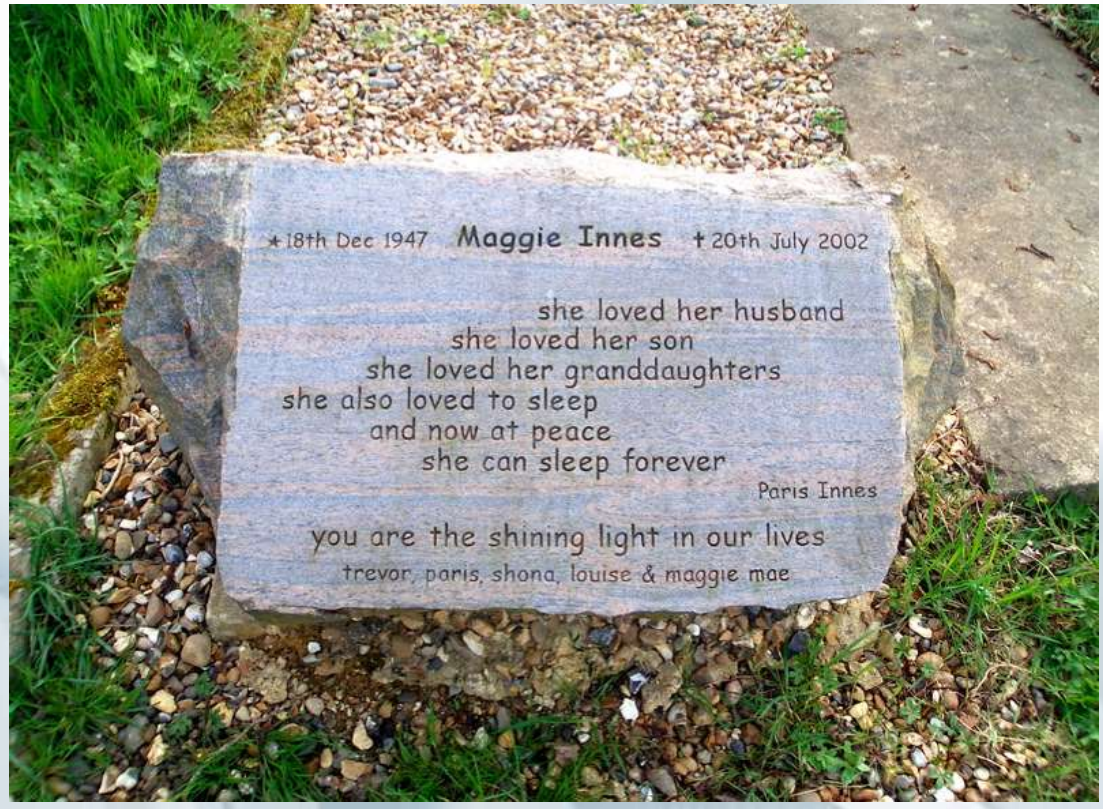
- Les inondations en Thaïlande réduise la production de disques durs
  - -30% ce mois-ci
    - http://www.linformaticien.com/actualites/id/22066/les-inondations-en-thailande-reduisent-de-30-la-production-de-disques-durs.aspx
- De la poudre RFID
  - Mais à quoi cela peut-il servir ?
    - http://pinktentacle.com/2007/02/hitachi-develops-rfid-powder/
- Oracle rachète RightNow pour $1,5 milliard
  - Un service de CRM en mode "Cloud"
    - http://www.computerworld.com/s/article/9221133/Oracle_buys_RightNow_for_about_1.5B

# Divers

- Dennis Ritchie est mort
  - Co-inventeur du langage C et du système Unix
    - http://www.lesnumeriques.com/dennis-ritchie-mort-news-21553.html
- John McCarthy est mort
  - Inventeur du langage LISP
- La série "The IT Crowd" s'arrête
    - http://www.theregister.co.uk/2011/10/24/it_crowd_shuts_down/
- Telnet #fail
    - http://boingboing.net/2011/09/25/747s-as-flying-unix-hosts-scada-in-the-sky.html

# Divers

- Andry Birds … sur Nokia ☺
- Enterré … en Comic Sans MS




# Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 13 décembre 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