Visual PC&Internet Security

 04 2006

EDITO

Bonjour chers internautes,
Dans cette édition du bulletin de sécurité 01/2005 vous trouverez une sélection de mes derniers tutoriaux (cours gratuits online) sur la "Sécurité PC&Internet". Le PC&Internet vous serons expliqués d'une manière transparente et non technique (VISUAL PC&INTERNET) !

SOMMAIRE

Il n'y a pas de problèmes, seulement des solutions.

Ensemble, nous trouverons la solution adéquate !

Mail : adcoet@pt.lu

Url : http://www.internetmonitor.lu

Browsers (FR) : Vulnérabilités multiples dans Firefox, Mozilla Suite,

Gust MEES

Neuf vulnérabilités dont plusieurs de niveau critique ont été découvertes dans les navigateurs Firefox et Netscape, la suite Internet Mozilla et le logiciel de messagerie Thunderbird. Certaines de ces failles permettent à un individu malveillant de prendre le contrôle à distance de l'ordinateur de sa victime ou à un virus de s'exécuter automatiquement via notamment une page web ou un courrier électronique piégé.

LOGICIELS CONCERNES :

Security News (FR) : La sécurité informatique au Luxembourg

Gust MEES

Selon les résultats de l'enquête communautaire sur l'utilisation des TIC et du commerce électronique dans les entreprises en 2005, le STATEC en collaboration avec le CEPS/INSTEAD, sous l'égide d'EUROSTAT, présente le rapport suivant :

Afin de protéger leurs systèmes informatiques 94% des entreprises connectées à Internet avaient installé en janvier 2005 des vérificateurs de virus ou des logiciels de protection, 63% disposaient de serveurs sécurisés, 72% de pare-feu et 55% de dispositifs de sauvegarde de données.

Malgré ces précautions un quart des entreprises connectées ont déclaré avoir connu des problèmes de sécurité informatique. Parmi ces entreprises 86 % ont été victimes d'attaques de virus aboutissant à une perte d'information ou de temps de travail.

Quelque 11% se sont plaints d'accès non-autorisés à leur système informatique ou à leurs fichiers et 2,3% ont été victimes de chantage ou de menaces au sujet de leurs données ou de leurs logiciels.

Remarque de la rédaction : des chiffres qui obligent à penser et à agir !

Source de l'article : eLuxembourg
http://www.eluxembourg.lu/actualites/2006/01/tic_entreprises_2005/stnews_4_2006.pdf

Tutoriaux (didacticiels) : C'est quoi un 'bogue' (bug) ?

Gust MEES

Le mot „bug" (bogue) est dérivé bien entendu de l'anglais et signifie „punaise" (Ungeziefer).
Mais, d'où vient cette signification qui à priori n'a rien en commun avec l'informatique ? Pour comprendre cette expression il nous faut retourner dans les années quarante où les premiers ordinateurs fonctionnaient encore avec des relais. Or, les relais fonctionnent avec des contacts, qui eux, ouvrent et ferment des circuits électroniques et/ou électriques.

Apparemment en 1945, à l'université de HARVARD l'ordinateur „MARK I" avait eu une panne de hardware (à l'époque il n'existait pas encore de software) qui était due à une mite. Cette mite s'était égarée entre des contacts de relais et provoquait ainsi un court circuit. L'ordinateur tombait en panne et les techniciens écrivaient dans leur rapport qu'il y avait un „bogue" qui était responsable du mauvais fonctionnement de l'ordinateur.

De nos jours quand il y a une anomalie dans un ordinateur le synonyme de „bogue" (bug) est utilisé pour décrire la cause, de même quand il y a des problèmes de programmation dans un logiciel (software).

Des problèmes de programmation dans un logiciel ?

Il n'y a pas de logiciels au marché qui ne renferment aucun bogue ! Selon une étude de la „TU-MÜNCHEN" http://www.tu-muenchen.de/jshpchooser.tupl les bogues sont inévitables. Un logiciel normal composé de mille lignes de programmation contiendrait 25 bogues (2,5 % de quota d'erreurs). Un logiciel de bonne qualité produirait encore 2-3 bogues (0,25 % de quota d'erreurs) et des logiciels spéciaux, programmés par exemple pour des applications militaires et spatiales reproduiraient encore un bogue sur dix mille lignes de code programmées (< 0,1 % de quota d'erreurs) !
http://www.decus.de/events/frankfurt/2004/vortraege/Software_Problems.pdf

Des logiciels de très bonne qualité ont malheureusement leur prix. On estime 1000 US $ par ligne de programmation, sans compter les tests de fiabilité et de sécurité qui à eux, sont estimés à 1600 € - 10000 € par mille lignes de code de programmation !
Imaginez-vous maintenant des logiciels qui contiennent quelques millions de lignes de code de programmation, comme c'est le cas des softwares de MICROSOFT®, MAC® et LINUX®. Il est évident qu'il y a des centaines, voir des milliers de bogues qui se produisent. Pour „déboguer" (debugging) toutes ces erreurs, il faudrait un investissement de temps et un budget énorme. Or, la concurrence ne dort pas et le produit final du logiciel doit apparaître au plus vite sur le marché pour se rentabiliser et de se faire remarquer (promotion) au plus vite avant la concurrence !
C'est pour cette raison que MICROSOFT®, MAC® et LINUX® proposent des „updates", des mises à jour (patches) pour enlever certains de ces bogues. Ces bogues, entre autre, sont responsables aussi pour les trous de sécurité (vulnérabilités) !

L'être humain n'est pas parfait, bien au contraire ! Toute chose programmée par un être humain ne peut être par conséquence parfaite non plus !
Maintenant vous comprendrez peut être un peu plus pourquoi il est plus que nécessaire pour faire les „updates" (mises à jour / patches) de chez MICROSOFT®, MAC® et LINUX® !

Comment et quand faire les updates de chez MICROSOFT®, MAC® et LINUX® ?
En principe MICROSOFT® publie chaque 2ème mardi du mois des correctifs. MAC® et LINUX® à eux publient aussi des „updates" mais sans dire que ce sont des mises à jour critiques, soit disant comme complément, contrairement à MICROSOFT® qui maintient une politique honnête vis-à-vis de sa clientèle.
Politique honnête ? Oui, en informant sa clientèle qu'il y a des vulnérabilités, MICROSOFT® au moins à ce point là est correct !
Bien au contraire pour les autres fabricants de systèmes d'exploitation, qui à eux, ne disent pas clairement spécifié pourquoi il faut télécharger les „updates". Ils mentionnent bien qu'il y a des mises à jour de disponibles, mais n'informent pas assez clairement les utilisateurs que c'est un „must" de les télécharger ! On pourrait croire qu'il existe une sorte de politique de dissimulation qui est pratiquée pour cacher que leurs produits sont aussi vulnérables !

Vous pouvez télécharger le didacticiel complet à l'adresse suivante :
C'est quoi un bogue ?

http://www.internetmonitor.lu/download/est_quoi_un_bogue.pdf

MAC (FR) : Plusieurs 'updates' de MAC à installer

Gust MEES

Plusieurs updates de sécurité MAC pour TIGER et PANTHER sont à installer, MAC les signe "recommanded", ce qui veut dire qu'il sont à risque de sécurité, à voir "vulnérabilité" !

Voici le lien pour télécharger les mises à jour critiques :
Security Updates MAC
http://www.apple.com/support/downloads/

Internetstuff Ettelbruck : Contrôle de sécurité gratuite des ordinateurs

Gust MEES

**
Les visiteurs de l'Internetstuff ayant s'inscrit comme membre par l'intermédiaire de la carte de membre (40 € / année pour les adultes et 20 € / année pour les jeunes et étudiants), peuvent dorénavant bénéficier d'un nouveau service.

**
**Ils peuvent faire contrôler leur ordinateur sur des risques de sécurité gratuitement (1 x par année) !
**

Bonjour chers internautes.
Adresse URL de notre Internetstuff:
http://www.ettelbruck.lu/internetstuff

Je vous souhaite bonne lecture, passez une journée agréable et à la prochaine.Gust MEESGérant Internetstuff EttelbruckFormateur pédagogique (avec un) TIC

Quoi de neuf à l'Internetstuff ?

Ce contrôle se compose d'un contrôle de vulnérabilités avec le logiciel MBSA (Microsoft Baseline Security Analyzer), contrôle de mise en place du SP2, réglages de sécurité de l'Internet Explorer et le cas échéant éradication des malwares trouvés.
Ensuite il sera procédé à l'installation de deux antispywares gratuits (Spybot Search&Destroy et Ad Aware) ainsi qu'un scan complet et immunisation avec ces logiciels. L'installation d'un antidialer et antimalware, tel que "A squared" arrondiront l'offre gratuite.
Les membres recevront un rapport contenant des screenshots

(captures d'écran) de l'analyse de leur ordinateur ainsi qu'une initiation à la "Sécurité PC&Internet". En plus ils cseront initiés à l'utilisation des logiciels installés sur leur ordinateur.
De cette manière nos membres bénéficierons d'un support maximum pour sécuriser leur ordinateur et notre "communauté" (Internetstuff) apportera sa part du gâteau pour un Internet plus sécurisé !
Permettez-moi de vous dire que cette action est plus que nécessaire ! Ayant inspecté déjà trois ordinateurs je dois dire franchement que j'ai été effrayé des resultats obtenus !
Un ordinateur d'un jeune de treize ans ne comportait pas moins de 251 virus, keylogger, browser hijacker, troyens et d'autres bestioles informatiques...

Tutoriaux (didacticiels) : MICROSOFT BASELINE SECURITY ANALYZER 2

Gust MEES

MICROSOFT BASELINE SECURITY ANALYZER 2

Le „MBSA“ de chez MICROSOFT® est un outil d'analyse de sécurité de votre ordinateur. Le logiciel MBSA vous permet de rechercher les erreurs de configuration de sécurité sur les ordinateurs exécutant MICROSOFT WINDOWS® SERVER 2003, WINDOWS XP ou WINDOWS 2000. Vous devez disposer des droits d'administrateur sur les ordinateurs que vous analysez !

Vous pouvez télécharger ce logiciel puissant et gratuit à l'adresse suivante :
MBSA (FR)

L'interface du MBSA nous montre les résultats suivants :

1. Nom de l'ordinateur
2. Adresse IP
3. Nom du rapport de sécurité
4. Date d'analyse
5. Analysé avec MBSA version 2.0.5029.2
6. Évaluation de la sécurité
7. Résultats de l'analyse des mises à jour de sécurité

Téléchargement (download) du didacticiel

Security News (FR) : L'Australie déconnecte les PC infectés

Gust MEES

En Australie, une agence gouvernementale et cinq fournisseurs d'accès Internet participent à un projet pilote visant à éliminer les PC zombies.

Le programme Australian Internet Security Initiative a été développé par l'Australian Communications and Media Authority (ACMA) et compte sur la collaboration de cinq fournisseurs d'accès Internet de l'Australie.

Les PC zombies - des ordinateurs préalablement infectés par un ver informatique ou un cheval de Troie - sont exploités à distance par des pirates informatiques ou des polluposteurs, notamment pour lancer des attaques par déni de service ou des campagnes de courriels indésirables. En outre, ces opérations sont presque toujours réalisées à l'insu des propriétaires de PC zombies, qui sont souvent les premiers surpris d'apprendre que leur ordinateur est employé de la sorte.

Dans un premier temps, le projet de l'ACMA identifiera donc, à l'aide des adresses IP, les PC zombies localisés en Australie puis transmettra la liste de ces ordinateurs aux fournisseurs concernés, car ce sont eux qui procurent cette adresse à leurs clients.

Les FAI participants s'engagent ensuite à contacter les propriétaires des PC infectés pour leur indiquer la façon de corriger la situation. Le communiqué de l'ACMA souligne que si un client ne répond pas à la demande du fournisseur, celui-ci pourrait aller jusqu'à déconnecter l'ordinateur zombie jusqu'à ce que le problème soit réglé.

Source de l'article : BRANCHEZ-VOUS (CA) http://www.branchez-vous.com/actu/05-11/09-333105.html

Linux (FR) : Un nouveau ver exploite des failles de Linux

Gust MEES

Un nouveau ver exploite les failles de sécurité des logiciels de serveurs Web du système d'exploitation Linux, peut-on lire dans un communiqué de McAfee publié Lundi.

Le ver nommé "Lupper" fonctionne en attaquant aveuglément les serveurs Web à la recherche d'une porte d'entrée où il pourra copier un autre ver et ainsi permettre à une personne malveillante de prendre le contrôle de l'ordinateur.

Trois failles de Linux comportent des risques plus élevés d'être contaminés par Lupper: une faile du système XML-RPC qui affecte surtout les outils pour gérer les blogues ou les sites Wiki; une faille du logiciel d'analyse AWStats; et un script du logiciel Webhints Remote Command Execution de Darryl Burgdorf.

McAfee considère tout de même que les risques d'être contaminés par Lupper sont faibles puisque le ver n'est pas encore répandu. Symantec, principal compétiteur de McAfee, considère toutefois que les risques d'être attaqué par ce vers, que Symantec préfère appeler "Plupii" sont plutôt moyennement élevés.

Source de l'article : BRANCHEZ-VOUS (CA) http://www.branchez-vous.com/actu/05-11/09-333101.html

L'oeil critique : Le problème de la sécurité et les utilisateurs...

Gust MEES

Est-ce que votre ordinateur est assez sécurisé, ou est-ce que cela vous laisse indifférent ? Franchement, je crois que la plupart des utilisateurs sont même inconscients des dangers et/ou indifférents et que ce leurs est même égal si leur ordinateur est assez sécurisé ou pas !

Avec le slogan "J'ai payé pour la bécane, alors il faut que cela fonctionne aussi correctement !" la plupart des internautes naviguent sur Internet. Malheureusement cette attitude est complètement fausse, mais à qui en vouloir !

Ne serait-il pas la responsabilité des revendeurs d'ordinateurs à veiller à ce qu'un ordinateur ne sorte de leurs lieux après avoir vérifié les paramètres suivants :

Est-ce que le SP2 (pour WINDOWS® XP) est installé ?
Est-ce que tous les "updates/patches" de MICROSOFT® sont installés ?
Est-ce qu'un pare-feu (firewall) de préférence un autre que celui de MICROSOFT® est installé ?
Est-ce qu'un antivirus est installé ?
Est-ce qu'un antispyware est installé ?
Est-ce qu'un antimalware est installé ?
Est-ce qu'un filtre parental est installé (pour un ordinateur familial) ?
Est-ce que l'activation de WINDOWS® a été faite ?

Ayant respecté ces quelques critères, qui d'ailleurs peuvent être employés comme argument de vente honnête (le service avant tout) :

Votre ordinateur est configuré de telle façon qu'il est protégé au maximum (à l'heure et la date actuelle) contre les attaques "actuelles".

Les revendeurs peuvent conseiller des logiciels payants antimalware à leurs clients, tels que des suites intégrants antivirus, firewall (pare-feu), antispyware, filtre parental et antispam.

Après livraison de l'ordinateur, un entretien de conseils en ce qui concerne la sécurité et la vigilance s'imposerait avec en finale la remise d'une brochure expliquant les démarches nécessaires à faire pour garder l'ordinateur sécurisé.

Est-ce trop demandé ? Honnêtement, je ne crois pas ! De nos jours nous exigeons aussi plus de sécurité pour nos voitures, tels que "airbag", "sip", "abs", etc. Les ordinateurs, eux aussi, devraient être munis d'airbag, abs, etc. en forme de logiciels, tels que décrit ci-dessus !

En ce qui concerne le contrôle technique, les F.A.I. (I.S.P.) devraient jouer un rôle plus important, c-à-dire : les ordinateurs infectés et non sécurisés, les "PC zombies" devraient être isolés de l'Internet afin de ne plus être opérables par les "botnets", à ne plus servir à la "mafia informatique" pour faire des actions illégales !

On pourrait même imaginer un "Label de qualité revendeur" émis par exemple par les ministères de l'Économie et/ou par la Commission Européenne et/ou organisation similaire.

Pour les revendeurs ceci impliquerait de bonnes connaissances dans la matière de sécurité PC&Internet, ce qui donnera en même temps confiance aux acheteurs d'ordinateurs et ce serait un excellent argument de vente pour la qualité de service du revendeur !

Qu'en pensez-vous ? Faites-nous savoir votre opinion par l'intermédiaire du formulaire ci-dessous.

Gust MEES (LU) / Formateur pédagogique TIC

Éditorial :
Internet Monitor agrandit sa palette de services

Gust MEES

M'occupant depuis l'année 2000 sérieusement de la „Sécurité PC&Internet" et donnant aussi des cours sur la matière, je dois reconnaître honnêtement et malheureusement que la plupart des gens restent indifférents à la vigilance, malgré des efforts des gouvernements et de la commission européenne.

Heureusement il y a quand même des personnes qui s'intéressent à la matière, comme vous, chers lecteurs.

En dehors des didacticiels gratuits (tutoriaux / cours pédagogiques) que je fournis sur notre site "Internet Monitor", je viens de créer de nouveaux menus de navigation que vous trouverez désormais sur le côté droite de notre site. Ces nouveaux menus vous offrent la possibilité de naviguer directement sur les sites des fabricants de logiciels de sécurité et/ou des fabricants de logiciels antimalwares, tels que "antispywares, firewall, etc.".

Très intéressant aussi sont les sites de "Belarc Advisor" et "MBSA" qui vous renseignent sur la conformité de l'état de sécurité de votre ordinateur. Pour les plus avancés, je vous conseille d'essayer "Process Explorer", un logiciel gratuit vous montrant tous les processus tournant sous WINDOWS®. Avec "Process Explorer" il vous sera possible de vérifier qu'il n'y a pas de programme malicieux lancé.

Prochainement je vous présenterais un didacticiel sur l'installation et l'utilisation du MBSA (MICROSOFT BASELINE SECURITY ANALYZER).

En plus vous y trouverez aussi un menu déployant sur la partie gauche en haut de notre site qui vous indique les liens directs envers les fabricants de systèmes d'exploitation MICROSOFT®, LINUX® et MAC® OS. Vous y aurez accès direct aux dernières mises à jour (updates/patches), logiciels spéciaux, forums, etc.

Notre "Internet Monitor" vous offre désormais les services suivants :

Didacticiels gratuits.
Newsletter (lettre d'information) gratuit.
Fiches pratiques gratuites.
Nouvelles du monde informatique gratuites.
Tests online (antivirus et port scan) gratuits.
Syndication de contenu professionnel et gratuit par l'intermédiaire de fils RSS.
Assurance de qualité grâce à nos partenariats officiels avec le ministère de l'Économie luxembourgeois (projet CASES / http://www.cases.lu) et le ministère de l'Éducation nationale luxembourgeois http://www.myschool.lu et http://www.mysecureit.lu.
Informations sur la protection des mineurs.
Glossaire (vocabulaire technique de l'informatique) entièrement créé par nos participants aux cours.
Annuaire de liens (Linklist).
Présentation de livres et booklets éducatifs sur la sécurité (DE, FR, EN)

Avec une certaine fierté je crois pouvoir dire qu'avec notre "Internet Monitor" vous avez un outil puissant à vos mains qui peut vous éviter pas mal de pépins si vous suivez bien nos conseils.

Néanmoins, si vous avez des suggestions et questions, n'hésitez pas à nous contacter via le formulaire "Contact". Nous sommes ouverts à toutes propositions, critiques constructives et commentaires.
Gust MEES / Formateur pédagogique T.I.C. (LU)

MAC (FR) : Apple met à jour Mac OS X pour réparer plusieurs vulnérabilités

Gust MEES

Apple a publié lundi une mise à jour importante de son système d'exploitation Mac OS X pour réparer des vulnérabilités de quatre composantes dont une qui pourrait être exploitée par des pirates, peut-on lire sur le site de la compagnie.

La mise à jour 10.4.3 concerne le noyau (kernel) du système d'exploitation, le "Finder", le logiciel de gestion des mises à jour ainsi

que les réseaux. Cette mise à jour est destinée à Mac OS X 10.4.2 et Mac OS X Server 10.4.2.

La faille la plus importante concerne la gestion des membres d'un réseau dans Mac OS X Server. Dans certaines situations, un membre authentifié peut ainsi revenir après qu'il ait été effacé de la liste des membres. Cette faille ouvre la porte à des personnes malveillantes qui peuvent aller chercher des données sans autorisation.

Vous pouvez télécharger la nouvelle mise à jour sur le site d'Apple.
Source de l'article : BRANCHEZ-VOUS (CA) http://www.branchez-vous.com/actu/05-11/09-331901.html

Vocabulaire d'Internet (FR) : C'est quoi un „splogue“ ?

Gust MEES

Le mot „splogue“ est dérivé des expressions anglaises „spam“ et „weblog“. Un „splogue“ est créé à partir d'un scripte placé sur le „blogue“ (blog, weblog) de son créateur. Ce scripte est programmé de telle manière qu'il vole le contenu d'autres blogues (blogs, weblogs) et qu'il publie son contenu ensuite sur le blogue de son créateur.

Sur ce même site sont créés aussi des liens à charactère publicitaire, des liens à promouvoir certains sites. Le but de cette opération est le bon positionnement dans les moteurs de recherche en augmentant le nombre de visites par l'intermédiaire des cliques.

Un bon positionnement dans les moteurs de recherche assure plus de visites de ces sites. Les créateurs de ces "splogues" sont ensuite payés par clique. Chaque fois qu'un site a été visité par l'intermédiaire du "splogue", son créateur sera crédité de quelques centimes.

Copyright (C) by Gust MEES (LU)

Copyright (FR) : Près de 15.000 «pirates» de musique au tableau de chasse de la RIAA

Gust MEES

L'industrie américaine du disque annonce une nouvelle vague de 757 plaintes, ce qui porte à environ 14.800 le nombre d'internautes américains poursuivis pour piratage de musique dans les réseaux d'échange de fichiers.

Les fermetures récentes de réseaux d'échange de fichiers (WinMX et Edonkey), qui s'appuient sur le jugement de la Cour suprême des États-Unis contre Grokster, ne diminuent apparemment pas l'ardeur avec laquelle la RIAA (Recording Industry Association of America) continue de poursuivre les particuliers suspectés de piratage de musique sur Internet.

Dans cette dernière vague de poursuites, la RIAA a indiqué que des utilisateurs P2P de dix-sept campus d'universités américaines font partie des 757 internautes soupçonnés d'avoir offert en partage un nombre considérable de fichiers audio.

Comme le veut la coutume, ces individus ne sont pour l'heure identifiés que par l'adresse IP de leur ordinateur à l'instant fatidique où ils ont été repérés par les enquêteurs la RIAA.

«Ceux qui continuent de s'adonner à ce vol en ligne menacent directement la capacité de la communauté musicale d'investir dans de nouveaux groupes et de la nouvelle musique que les amateurs voudraient entendre. Ces poursuites constituent une partie importante de notre défense contre cette menace», explique Cary Sherman, présidente de la RIAA.

Source de l'article : BRANCHEZ-VOUS (CA)
http://www.branchez-vous.com/actu/05-09/09-297503.html

MAC (DE) : Sicherheits-Update für Mac OS X

Gust MEES

Apple bietet für Mac OS X 10.3.9 (alias Panther) und 10.4.2 (alias Tiger) einen wichtigen Sicherheits-Patch an, der gleich mehrere Lecks stopft.

Das Mac-Update 2005-008 behebt unter anderem Anfälligkeiten in den Komponenten Mail, QuickDraw, Login-Fenster, QuickTimeJava und Safari. Eine Installation empfiehlt sich also. Der ca. 7 MB schwere Download ist entweder über die automatische Softwareaktualisierung von Mac OS X oder die Apple-Website erhältlich.(sz)
http://www.apple.com/support/downloads/
Quelle des Artikels: PC TIPP (CH) http://www.pctipp.ch/webnews/wn/31292.asp

MAC (FR) : 44 correctifs pour le Mac OS X

Gust MEES

Apple vient de rendre disponible plus de 44 correctifs, dont plusieurs critiques, destinés à corriger des failles de sécurité de son système d'exploitation Mac OS X.

Qu'on se le dise. Les failles de sécurité ne sont pas que l'apanage de Windows. Les utilisateurs des systèmes d'exploitation Linux et le Mac OS X sont aussi confrontés à ces problèmes.

C'est d'ailleurs la raison pour laquelle Apple a rendu disponible hier une série de 44 correctifs conçus pour colmater certains trous de sécurité.

De ce nombre, plusieurs sont destinés à corriger des failles critiques, dont des attaques par débordement de mémoire tampon (buffer overflow). Le fureteur Safari bénéficie lui aussi d'un correctif visant à empêcher l'exécution d'un code arbitraire via un simple clic sur un hyperlien.

Certaines applications à code source libre utilisées par le Mac OS X, tel le serveur Web Apache 2, le logiciel d'authentification Kerberos et le service d'impression CUPS, ont elles aussi reçu leurs correctifs. Les utilisateurs du système d'exploitation Mac OS X peuvent lancer le service de mises à jour intégré à l'OS pour installer ces correctifs. Il est aussi possible de récupérer un fichier correcteur sur le site d'Apple.
Source de l'article : BRANCHEZ-VOUS (CA)
http://www.branchez-vous.com/actu/05-08/09-274903.html