L'Actu Sécurité n°8

XMCO Partners

PLAN

"La politique de sécurité, à quoi ça sert ? "

Bonjour.

Il y a 10 ans, la définition d'une politique de sécurité représentait près d'une demande de prestation sur deux. Un engouement si fort que certains cabinet étaient devenus à l'époque les vrais spécialistes de la politique de sécurité. Facile de revendre et revendre toujours le même document....

Qu'en est-il aujourd'hui ? A en croire mes interlocuteurs, tous les grands groupes, ou presque en sont dotés. Quelques PME en ont une, quant aux petites entreprises, c'est un sujet qui fait parfois rire.

Mais finalement, 10 ans après, le retour sur investissement de tous ces efforts semble très difficile à mesurer. Pourquoi ? Tout simplement parce que personne n'avait, à l'époque, la moindre idée de ce à quoi une politique de sécurité pouvait servir... Il en fallait une, certes, mais certainement pas un document long, obscur et totalement inutile comme on le constate souvent.

De même, qu'en est-il des tableaux de bords sécurité dont tous les Responsables Sécurité et tous les dirigeants rêvent ? Pas grand chose à l'horizon... Il faut reconnaître que nous travaillons dans l'un des domaines les plus flous de l'informatique et admettre que rien n'a été fait pour standardiser les différentes démarches et faciliter ainsi l'appréhension des enjeux de la sécurité dans les entreprises. L'échec dans ce domaine est, d'ailleurs, en partie responsable de la négligence de la sécurité.

Qu'aurait-il fallu faire ? D'après moi, il aurait fallu prendre le problème à l'envers, et demander aux responsables fonctionnels ce qu'ils voulaient surveiller et mesurer. De cette manière, il aurait été possible de définir un objectif ou une destination. Lorsque l'on sait où on va, trouver le meilleur chemin est toujours plus facile que lorsqu'on avance à vue...

Et maintenant, que faut-il faire ? Redéfinir tout simplement les objectifs pour atteindre les buts que nous nous étions fixés il y a 10 ans à savoir: faire de la sécurité un centre de profits !

Marc Behar

1. LES CAHIERS DE L'OWASP

LA GESTION DES SESSIONS

Dans cette rubrique, nous étudierons un des sujets présentés dans le guide OWASP (The Open Web Application Security Project). L'OWASP est un guide qui présente les points majeurs à respecter afin de renforcer la sécurité des applications.
Nous avons choisi de vous présenter la première partie du chapitre relatif à la gestion des sessions. Les applications web dynamiques doivent utiliser un mécanisme afin de gérer au mieux les sessions des utilisateurs connectés. Une mauvaise implémentation de ce point peut avoir des conséquences importantes et augmenter les risques de piratage.
Cet article abordera les points essentiels ainsi qu'un aperçu des règles et des meilleures pratiques afin d'assurer la sécurité des sessions.

XMCO | Partners

OWASP
The Open Web Application Security Project

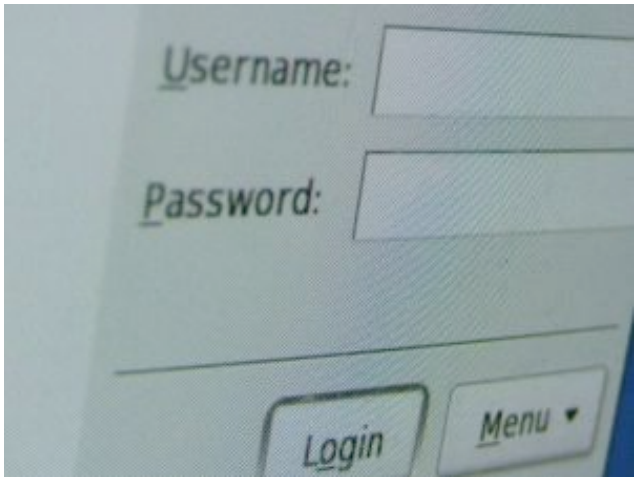
La sécurité des sessions

Objectifs

La sécurité d'un site web repose sur de nombreux points. La gestion des session et, notamment, la solidité et la confidentialité de ces dernières constituent les principaux enjeux qui permettent de définir le niveau de sécurité de l'application. Il est donc impératif que les développeurs prennent conscience de la nécessité d'assurer un contrôle permanent de l'authentification et d'assurer la robustesse de l'application face aux rejeux de paquets, aux requêtes forgées et aux insertions illicites dans les communications (man-in-the-middle).

La gestion des sessions

Alors que les programmes traditionnels stockent les données locales en mémoire allouée par le système d'exploitation sous la forme de variables dans la mémoire pile, les applications web sont basées sur un mode de fonctionnement différent. Le serveur renvoie simplement une page déterminée en fonction de la requête du client.
Afin d'assurer l'étanchéité des utilisateurs et de garder l'état du client connecté, les serveurs Web utilisent de plus en plus les plates-formes de développement comme J2EE ou ASP.NET,. Ces framework implémentent des mécanismes de maintient de session qui permettent de maintenir chaque utilisateur dans une session bien définie.



Une information cryptographique aléatoire et unique, partagée entre le client et le serveur (dans un cookie ou directement dans l'url), est fournie par le client dans chacune de ses requêtes. L'application web peut ainsi simuler un mode de fonctionnement basé sur des états. La capacité de maintient des utilisateurs au sein de sessions uniques et étanches représente l'un des enjeux critiques pour la sécurité d'une application web.

Il est important de noter que certains langages comme Perl CGI sont dépourvus d'un tel mécanisme. Le développeur doit alors construire son propre mécanisme de conservation des sessions ce qui est coûteux et dangereux.
Les plates-formes de développement telles que J2EE, PHP, ASP et ASP.NET gèrent les problématiques "bas niveaux" de la conservation de session. Elles apportent, en parallèle, des possibilités de contrôle plus fin de la programmation plutôt que pour les configurations. (Ex : ASP.NET implémente la variable cachée « view state ». Cette dernière est résistante face aux manipulations (parameters tampering). Elle est aussi présente sous la forme d'un champ caché dans chaque page web).

La génération permissive des sessions

Beaucoup de plates-formes de développement (ou “framework”) génèrent automatique une nouvelle session si la requête cliente n’en possède pas. Ce comportement est appelé « génération permissive de session ». Couplé avec des attaques de type phishing et à un mauvais contrôle des autorisations, il est possible de réaliser des attaques dévastatrices.
La création de sessions doit donc être strictement contrôlée. Il est important de s’assurer qu’une session n’est pas déjà utilisée, qu’elle est bien dans l’état “déconnecté” et qu’aucun rôle ne lui est assigné par défaut. Ainsi un contrôle de validité de la session et de l’authentification doit être effectué avant tout affichage de contenu.

L’exposition des variables de session

Certaines plates-formes utilisent un répertoire partagé du serveur Web pour stocker les données de session. En particulier, PHP qui stocke par défaut ces données dans “/tmp” ou dans “C:\windows\temp” sur les systèmes Windows. Ces répertoires n’assurent pas la protection des données de session et peuvent conduire à la compromission de l’application si le serveur Web héberge plusieurs utilisateurs ou bien s’il est compromis.
Lorsque les sessions sont stockées sur le disque ou dans une base, il est important de savoir qui a accès à ces données. En outre, le serveur d’application doit être configuré de manière à utiliser un répertoire par application. Si ça n’est pas envisageable, un chiffrement des données de session est impératif.

Les algorithmes de génération de session

Tout système de session robuste doit être pourvu d’un générateur de session efficace.
Si le gestionnaire de session délivre des jetons prédictibles, un attaquant n’a même pas besoin de voler les variables de session d’un utilisateur – il lui suffit simplement de tester plusieurs numéros de session pour voler aisément la session d’un utilisateur. Il est important que les jetons de session (ou “session-ID”) soient uniques pour chaque utilisateur, non prédictibles et résistants au “reverse engineering”. Il est vivement conseillé d'utiliser des générateurs connus comme Yarrow ou EGADS [1].

Même un algorithme sécurisé, d’un point de vue cryptographique, peut être vulnérable à la prédication de sessions valides si l’espace de recherche est trop réduit. Un attaquant peut tout à fait construire un script de type brute-force afin d’essayer toutes les possibilités. Les jetons de session doivent donc être générés dans un espace de recherche suffisamment grand pour prévenir une éventuelle attaque par brute-force. Il est important, ici, de garder à l’esprit que les capacités de calcul et les bandes passantes vont encore fortement augmenter, avec pour conséquence directe de fragiliser les mécanismes de génération de jetons de session. Enfin, un bon jeton doit être constitué de tous les caractères possibles (imprimables), majuscules et minuscules compris.

La durée de vie et la fin des sessions

L’expiration des sessions

Les jetons de session qui n’expirent jamais laissent aux pirates une période de temps infinie pour deviner une session valide ou pour réaliser une attaque par “brute-force”. Par exemple, l’option « Remember Me » que l’on trouve sur beaucoup de sites de commerce en ligne : si le cookie ou le jeton de session d’un utilisateur est volé, un attaquant peut alors utiliser ce jeton statique pour voler le compte de l’utilisateur lésé. Le problème est particulièrement critique dans un contexte publique où les stations clientes sont partagées (cybercafés, écoles, etc.).
Par ailleurs, les jetons de session peuvent être potentiellement enregistrés (loggés) et mis en cache dans les proxies : si un attaquant prend le contrôle du proxy, toutes les sessions non expirées peuvent être volées par l’attaquant.
Les meilleures pratiques recommandent une utilisation de session (time out) de 5 minutes pour les applications à risque et de 20 minutes maximum pour les applications non critiques.

Le renouvellement des jetons de session

Afin de réduire le risque de vol de session ou d’attaque par brute-force, le serveur web peut, de manière continue et transparente, expirer et régénérer les jetons de session. Ce comportement réduit la fenêtre d’attaque pour les tentatives de vols de session ou d’attaques par brute-force.

Les renouvellements des jetons de session doivent être effectués :

- **Avant toute transaction critique.**
- **Après un nombre déterminé de requêtes.**
- **Après une période de temps définie (par exemple 20 minutes).**

Détection et prévention des attaques sur les jetons de session

La plupart des sites web possèdent des protections contre la tentative d'un grand nombre de mots de passe (par exemple, le site peut temporairement bloquer un compte ou bloquer l'IP de l'attaquant). Cependant, un attaquant peut, très souvent, tenter un très grand nombre de jetons de session avec une URL ou un cookie forgé sans être détecté. La plupart des systèmes de détection d'intrusion (IDS) ne protègent pas contre ce type d'attaque ; les tests d'intrusion ne portent généralement pas suffisamment d'égards à ce type de vulnérabilité, notamment pour les sites de commerce en ligne.

Différentes méthodes sont choisies. Certains ralentissent fortement ou bannissent carrément l'adresse IP de l'attaquant. Ce comportement peut engendrer des dommages collatéraux dans le cas où les fournisseurs d'accès Internet utilisent des caches transparents pour accélérer leurs services. (Pour cela, préférez toujours le contrôle de l'entête http proxy_via). D'autres préfèrent bloquer le compte si celui ci est défini. Enfin, un système de détection d'anomalie ou l'utilisation de modules spécialisés comme "mod_dosevasive" et "mod_security" pour les serveurs Apache peuvent s'avérer utiles.

La fermeture de session

Avec la popularité croissante des cyber-cafés et autres lieux de partage de connexion Internet, les jetons de session font face à un nouveau risque. En effet, un navigateur Internet ne détruit les cookies de session que lorsque le navigateur est complètement fermé. Dans la plupart des cas, les navigateurs restent constamment ouverts même après le départ de l'utilisateur.
La session de l'utilisation (côté client) doit être effacée et les cookies de session (coté serveur) écrasés dès que le client se déconnecte de l'application.

Les Meilleures Pratiques

La meilleure pratique ne consiste pas à réinventer la roue mais plutôt à utiliser un système de gestion de sessions robuste et standard. La plupart des environnements de développement web contiennent une API de gestion de session correcte. Cependant, les anciennes versions contenaient des vulnérabilités. C'est pourquoi il est fortement recommandé de toujours utiliser la version la plus récente de la technologie choisie (car plus performante) et de veiller aux publications de correctifs. Une recherche sur les moteurs de recherche ainsi que sur le site de l'éditeur vous permettra de définir la version la plus récente de votre plate-forme de développement.

Plusieurs précautions sont à prendre :

- Stocker les mots de passe et les profils dans le serveur et ne jamais transiter par le navigateur client.
- Faire transiter les paramètres de navigation via l'url si ceux-ci sont correctement validés et contrôlés par le serveur.
- Stocker les paramètres de présentation (comme le thème ou la langue) dans un cookie.
- Faire résider du coté serveur et ne jamais faire transiter dans les formulaires les données secrètes. Les données des formulaires ne doivent pas contenir d'informations secrètes ni cachées. Les champs cachés doivent être utilisés pour conserver des numéros de séquence et pour prévenir des attaques par brute-force (champs conservant le nombre d'essais).

Dans le cas des formulaires à plusieurs pages, les données peuvent transiter par le côté client dans les cas suivants :

- Lorsqu'un contrôle d'intégrité est strictement effectué.
- Lorsque les données sont contrôlées et validées après chaque page ou bien lors de la dernière soumission.
- Les données secrètes (comme les mots de passe ou les droits de l'utilisateur) ne doivent jamais être modifiables par le client (aussi bien en mode GET qu'en mode POST). Ces données doivent être conservées via un numéro de session.

Les sessions sont le point d'entrée d'attaques en tout genre que nous vous présenterons le mois prochain.

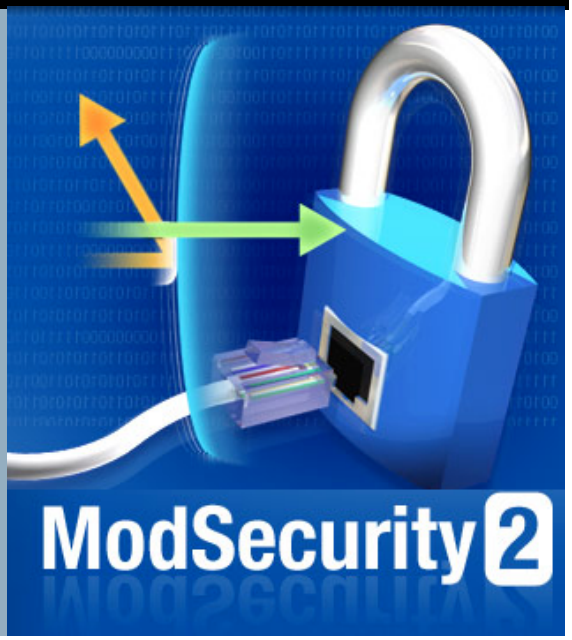
3. NOUVELLE TENDANCE

LE MODULE DE SECURISATION D'APACHE

L'ouverture des entreprises sur le monde via Internet est devenue un besoin incontournable. Malheureusement, la sécurité des applications n'est pas suffisamment prise en compte. Ainsi, plus de 70% des exploits publiés concernent une vulnérabilité liée à une application web. Devant ce constat alarmant, la société « Breach Security » a développé un module pour les serveurs web Apache afin d'améliorer sensiblement la sécurité de ces applications sans modifier l'architecture existante.

Mod_security permet de lutter contre les attaques classiques comme l'injection de commandes SQL, la lecture de fichiers sensibles, l'accès à des répertoires arbitraires, etc. Ce module apporte une couche de sécurité en amont des services web.

XMCO | Partners



Un accès facile pour un système complexe

Le principal avantage des services web réside dans la possibilité de partager certaines ressources de l'entreprise depuis n'importe quel accès Internet. Cependant, devant l'étendue des vecteurs d'attaques, la sécurité des applications web devient rapidement un empilement de solutions ou de méthodes qui corrigent certains problèmes tout en apportant de nouvelles vulnérabilités.
Par exemple, les ressources partagées correspondent parfois des données privées dont l'accès doit être restreint aux seuls utilisateurs autorisés. Les applications nécessitent donc de fournir un service d'authentification et d'autorisation afin de gérer les connexions entrantes. Or, ce mécanisme implique l'utilisation d'une base de données afin de stocker les informations des utilisateurs. Ce composant supplémentaire nécessite alors de prendre en compte des tentatives de contournement de l'authentification par injection de commandes SQL arbitraires au sein de la base de données ainsi que les tentatives d'exploitation de failles connues du serveur de base de données relationnelles.

La complexité et la sécurité de chaque élément des applications entraînent une escalade des technologies au sein de l'architecture web.

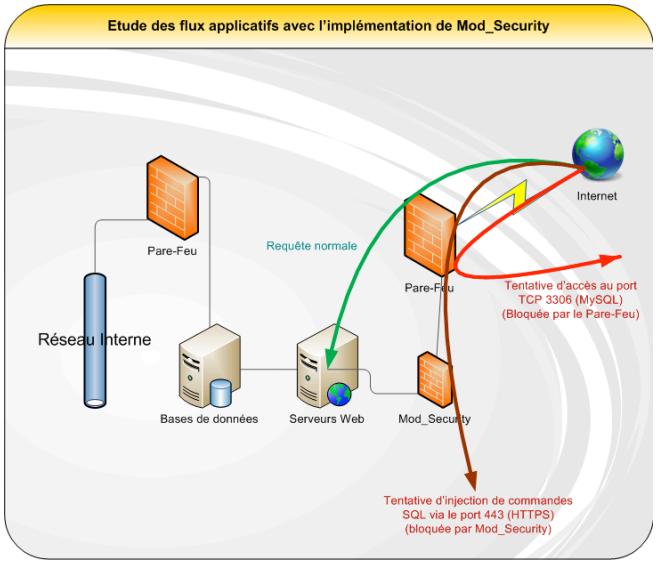
Les services web sont, aujourd'hui, devenus la cible privilégiée des pirates informatiques car les attaques ne nécessitent que peu de moyens : un simple accès Internet.

La sécurité de chaque composant de l'architecture est, généralement, partiellement implémentée ce qui conduit à un niveau global assez faible. Par conséquent, plus une application est complexe et plus l'attaquant a d'opportunités de trouver une faille de sécurité.

Les fausses idées reçues

Le pare-feu constitue un élément du réseau indispensable. Il permet de bloquer les attaques des couches basses du modèle OSI. Néanmoins, il ne protège pas l'application web. Les failles des services web sont dues à des erreurs liées à un comportement anormal de l'application, mais génèrent un trafic totalement légitime pour le réseau. Le pare-feu ne bloquera donc pas les flux d'un éventuel pirate.

L'implémentation du protocole SSL permet de remédier aux problèmes de confidentialité, d'intégrité et d'authentification des services webs. Ainsi, une entreprise et un utilisateur peuvent garantir leur authenticité et vérifier que les messages échangés ne sont ni altérés ni accessibles par une tierce personne. Or, les messages échangés peuvent exploiter une faille applicative ; l'utilisation de la cryptographie ne protège donc pas le service web.



Par ailleurs, il est courant de constater des services web exécutés sous des privilèges systèmes élevés, le plus souvent ceux de l'administrateur. Or, en exploitant une faille applicative, un pirate obtiendrait des privilèges élevés sur le serveur hébergeant le service. Il pourrait ainsi prendre le contrôle total de la machine. Dans la majorité des cas, un serveur applicatif n'a besoin d'aucun privilège particulier.

Le module "mod_security"

Les fonctionnalités

Ce module, open source et sous licence GPL, est destiné à renforcer la sécurité du service web et ce, directement par l'intermédiaire du serveur HTTP. Les principales opérations s'effectuent durant le traitement des entrées/sorties du serveur. C'est-à-dire, avant la prise en charge des données par l'application et après l'exécution du processus.

Toutes les requêtes entrantes sont ainsi analysées et traitées en amont afin de bloquer les techniques de contournement et d'encodage de caractères. Les paramètres fournis par les méthodes POST et GET sont interceptés et peuvent être journalisés dans leur globalité pour une analyse postérieure. Les données reçues sont étudiées afin de bloquer les débordements de tampon, la présence de « shellcode », l'accès en lecture à des fichiers sensibles et l'injection de scripts ou de commandes. Dans le cas où l'application permet de télécharger des fichiers sur le serveur, le module peut vérifier l'extension des fichiers et exécuter un script externe à l'instar d'un anti-virus.

Mod_Security permet également de filtrer les messages renvoyés au client afin de supprimer tous les messages d'erreurs trop explicites. En effet, ces messages contiennent souvent des informations précieuses qui aident un pirate à préparer son attaque.

Afin d'élever la sécurité globale du système, le module exécute automatiquement le serveur HTTP sous des privilèges restreints ainsi que dans un environnement limité (chroot). Cette solution permet de diminuer les impacts lors de l'exploitation d'une vulnérabilité non corrigée ou inconnue.

L'implémentation

Le module « Mod_Security » a été développé afin d'élever le niveau de sécurité global de l'application web sans repenser celle-ci.
L'implémentation de ce module ne nécessite qu'une simple modification du fichier de configuration du serveur HTTP Apache ainsi que le redémarrage du service.

Les lignes ajoutées au fichier de configuration permettent de paramétrer les filtres et les options souhaités.

Quelques exemples :

*Test de l'utilisation du module

```
<IfModule mod_security.c>
```

*Démarrage du processus de filtrage

```
SecFilterEngine On
```

*Filtrage des caractères d'entrées

```
SecFilterCheckURLEncoding On
SecFilterCheckUnicodeEncoding On
```

*Traitement des cookies

```
SecFilterNormalizeCookies
```

*Filtrage des caractères de sorties

```
SecFilterScanOutput On
```

*Filtrage du contenu des requêtes 'POST'

```
SecFilterScanPOST On
```

*Action par défaut : log & rejet

```
SecFilterDefaultAction
```

*Protection contre le "Directory Transversal"

```
SecFilter "\.\./"
```

*Protection contre l'injection de commande SQL de type "xp_cmdshell"

```
SecRule ARG:p "xp_cmdshell"
"t:urlDecode,t:lowercase"
…
</IfModule>
```

Par ailleurs, les entreprises qui ne disposent pas de serveurs HTTP Apache, peuvent implémenter cette solution en ajoutant un « reverse-proxy » à leur infrastructure afin de sécuriser et d'augmenter la disponibilité des applications webs.

Conclusion

Le module Mod_Security représente une solution pour les entreprises qui ne peuvent pas modifier aisément leurs applications web. Cet avantage permet de réduire les temps de déploiement mais surtout d'alléger le code source des applications, facteur de stabilité et de sécurité.

Bibliograpie

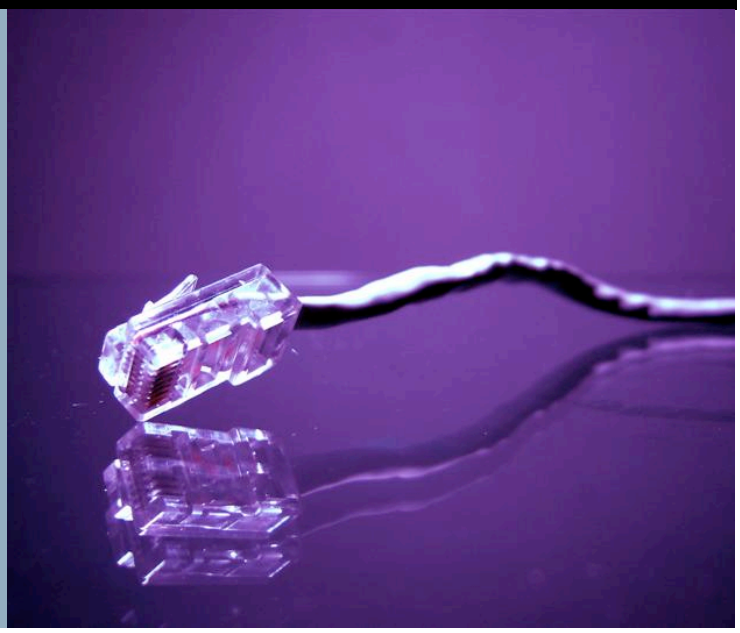
http://www.modsecurity.org/

3. DOSSIER SPECIAL : ADMINISTRATION A DISTANCE

PRESENTATION DES ACTEURS DU MARCHE

L'administration des serveurs est une tâche souvent laborieuse. Se déplacer sur le poste est coûteux en temps et en argent. Les logiciels de contrôle à distance sont, aujourd'hui, incontournables mais encore peu utilisés dans les entreprises. Petit tour d'horizon des solutions logicielles du marché….

XMCO | Partners



Un besoin réel

De nombreux logiciels d'administration à distance ont vus le jour ces dernières années. Ces outils, indispensables pour les administrateurs, apparaissent, peu à peu, dans les entreprises. Les particuliers et les supports en ligne commencent également à prendre conscience de la réelle utilité de ce genre de logiciels. Les utilisations sont diverses : possibilité de contrôler votre ordinateur personnel depuis votre bureau, démonstration de manipulations à un de vos collègues, et ce, en toute confidentialité si l'on couple ces logiciels à un tunnel SSH. En réseau local comme via Internet, il suffit de connaître l'IP de la machine à contrôler afin de pouvoir profiter de ses logiciels.

VNC et « **Bureau à distance »** intégré dans plusieurs versions de Windows ou **PC Anywhere**, sont les plus connus du marché. Ces trois logiciels répondent au même besoin, seuls leurs prix diffèrent…Nous vous présenterons, tour à tour, ces programmes aux résultats plus ou moins satisfaisants…

VNC
Description

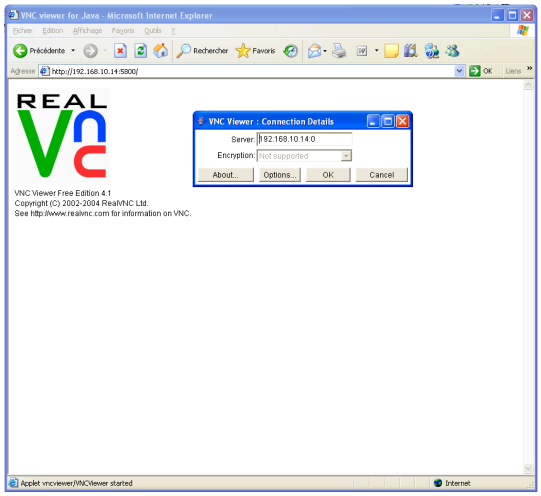
VNC ou Virtual Network Computing est un produit développé par les laboratoires AT&T de Cambridge et racheté par ORL. VNC est présenté officiellement par la société RealVNC depuis 2002. Il connaît un fort succès avec plus de 100 millions de téléchargements depuis sa création. Ce logiciel libre et gratuit, repose sur un mode « client » / « serveur ». Lors de l'installation, il est possible de choisir le mode à installer sur le poste cible. Le module « Server » devra impérativement être installé et démarré sur la machine à contrôler.
VNC est basé sur le protocole RFB pour Remote Frame Buffer. Le principe est simple. Le client interroge le serveur qui lui renvoie, via TCP/IP, des portions d'écran par paquets de rectangles (ou framebuffer updates). Le serveur répond, en réalité, sous la forme suivante : « insérer un rectangle de pixel à la position x, y ».
Les mises à jour sont ensuite envoyées par le serveur uniquement sur la demande du client. Ceci permet à ce dernier d'effectuer un contrôle plus subtil en fonction de plusieurs paramètres. Par exemple, la vitesse de transmission, qui lui permet d'estimer le meilleur taux de rafraîchissement selon l'encombrement de réseau. Parallèlement, le client envoie au serveur, toujours via TCP/IP, toute action qui a été effectuée sur le clavier ou sur la souris afin que ce dernier les répercute sur la machine sur lequel il tourne.

Toutes les plate-formes sont supportées (Unix, Mac, Windows). IL est ainsi possible de contrôler une machine UNIX à partir d'un client Windows. Par ailleurs, contrairement au bureau à distance de Microsoft présenté dans la suite de ce document, la session courante de l'utilisateur n'est pas interrompue.

Accès à un poste distant via le client VNC

Fenê

Par ailleurs, VNC peut être utilisé via une applet Java générée à partir d'un navigateur web. L'accès à votre machine distante, sans client VNC, est alors possible et simplifie l'administration sans installation préalable de logiciel.



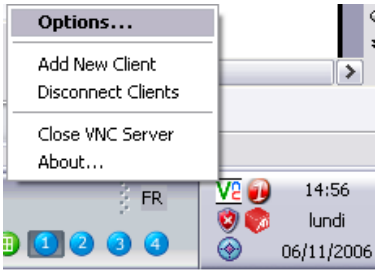
Accès à un poste distant via un navigateur web

Sécurité

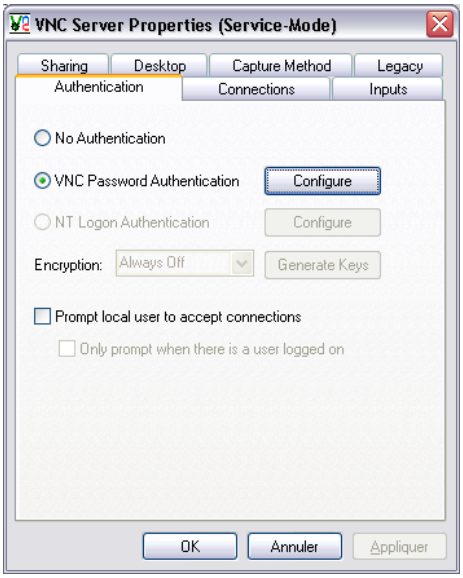
Le protocole VNC est efficace mais il n'est absolument pas sécurisé. Aucun chiffrement n'intervient sur aucune des couches du modèle OSI. Malgré tout, il peut être facilement utilisé avec un logiciel de tunneling comme SSH ou un programme VPN. Seules les versions « Ultra VNC » et « Real VNC » commerciales proposent l'utilisation de chiffrement sur la session.

Plusieurs failles de sécurité dont une critique, ont été identifiées. Un exploit doté d'un scanner afin d'identifier les machines vulnérables, a récemment été publié. Ce dernier permettait de prendre le contrôle de tous les postes possédant VNC version 4.1.1 avec une version de VNC Viewer modifiée. (voir bulletin XMCO n°1147765706).

Configuration



La configuration est extrêmement simple. Un mot de passe doit être défini sur le poste « serveur ». Le reste des options, installées par défaut suffit pour utiliser le logiciel. Il faut, bien entendu, ouvrir le port choisi (ou 5900 par défaut) sur le pare-feu de la machine cible.



Fenêtre de configuration de VNC "serveur"

Avantages

VNC se différencie des autres logiciels par sa gratuité, son inter-opérabilité multi-plateformes et sa taille réduite (150ko pour le viewer). Plusieurs versions existent et ciblent des besoins spécifiques (TightVNC est plus léger et possède peu de fonctions contrairement à Ultra VNC).

Inconvénients

Le trafic n'est pas chiffré. Cela peut être critique lorsque des informations confidentielles sont envoyées du client au serveur. De plus, le protocole VNC est relativement lent. Ce logiciel est à utiliser sur des réseaux locaux pour obtenir une qualité de service acceptable.

Bilan

VNC est un très bon logiciel qui peut être utilisé sur différentes plate-formes. Malgré tout, la lenteur du protocole limite considérablement son utilisation via Internet.

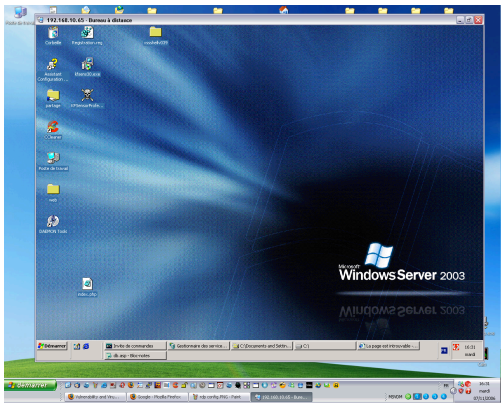
Bureau à distance

Description

Le «bureau à distance » de Windows est un service peu connu mais extrêmement efficace. Implémenté par défaut sur les versions XP PRO, 2000 et 2003, cette fonctionnalité permet également de contrôler des PC sur des distances plus longues. Vous pouvez tranquillement utiliser Internet pour diriger un PC qui se trouve à des centaines de kilomètres. En effet, le protocole RDP « Remote Destop Protocol » est basé sur le protocole ITU.T.share plus connu sous le nom de T.128.

La première version (4.0) fut implémentée pour la première fois sur la plate-forme Windows NT4. Elle est aujourd'hui utilisée par Windows Server 2003 en version 5.2.
Il suffit que le poste cible implémente le service « Terminal Serveur ».

De nombreuses fonctionnalités sont disponibles : affichage des couleurs 24 bits, support du son pour écouter les sons produits sur l'ordinateur distant, utilisation de l'imprimante locale pour les documents hébergés sur la machine distante, mapping des disques durs locaux.



Accès à un ordinateur distant (Windows 2003) via le "Bureau à distance"

Sécurité

Le trafic de ce protocole est intégralement chiffré avec l'algorithme RC4. Peu de failles ont été publiées. L'utilisation du Bureau à distance reste sécurisée.

Configuration

Aucune configuration préalable n'est requise. Les postes XP Pro, 2000 et 2003 implémentent cette fonctionnalité par défaut. Le port 3389 doit être ouvert sur le pare-feu afin de recevoir les connexions entrantes.
Sur le poste client, il suffit de cliquer sur « Démarrer » puis « Exécuter » et d'entrer « mstsc » afin d'obtenir la console.

Une fois l'adresse IP de la station cible entrée, il est possible de se logguer sur le poste distant.

Avantages

Le Bureau à distance utilise un protocole rapide qui permet d'administrer une station via Internet. Le protocole utilisé chiffre les données (clavier et activité de la souris). Un attaquant peut donc difficilement voler des informations confidentielles.

Inconvénients

Ce service est basé sur la session de l'utilisateur. Ce dernier est donc déconnecté dès qu'un accès distant est effectué.

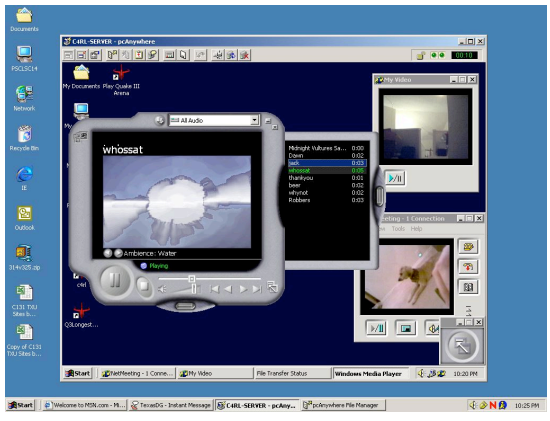
Bilan

Le « bureau à distance » est une fonctionnalité Windows parfaitement implémentée. La qualité des accès distant en font le logiciel d'administration le plus efficace. De nombreuses options (comme le partage des disques durs locaux) rendent ce logiciel incontournable.

PCAnywhere

Description

PcAnywhere est le troisième logiciel renommé du marché. Il propose les mêmes services que VNC et RDP. Il se différencie par des options et une configuration plus évoluée que celles des deux logiciels présentés ultérieurement.
Développé par Symantec, ce dernier se compose d'un fichier d'installation unique relativement lourd. Quatre options majeures sont accessibles dès le lancement du logiciel : « remote control » (accès distant, utilisation du client, « file transfer » (transfert de fichiers),



Accès à un ordinateur distant via PC Anywhere

« quick connect » (connexion rapide) ou « host » (lancement du serveur).

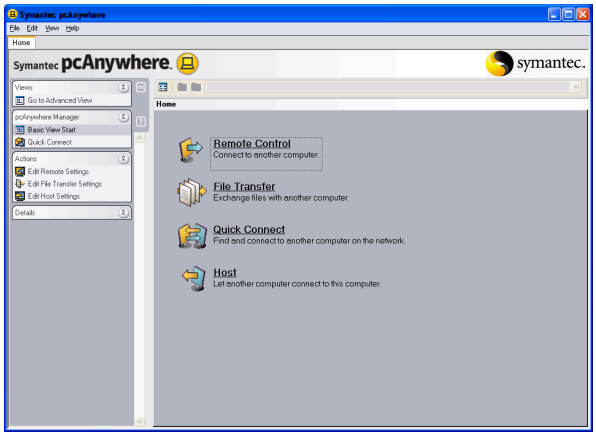
PCAnywhere structure son offre autour de fonctionnalités plus évoluées qui sont également présentes dans l'outil de Microsoft. Trois versions sont proposées : une pour les plate-formes Linux, une autre pour Windows et une dernière pour la plate-forme MAC OS X.

Sécurité

PCAnywhere utilise le chiffrement AES 256 bits pour sécuriser les accès distants ainsi que les transferts de fichier.

Configuration

La configuration est moins intuitive mais reste tout de même très simple. L'utilisateur doit cliquer sur l'option « host » présente sur le serveur. Puis, à partir du poste distant, accéder à la fonctionnalité "host" et suivre, pas à pas, les consignes afin de remplir l'adresse IP et les identifiants.



Avantages

L'avantage de ce logiciel, par rapport à VNC et RDP, est l'utilisation du client sur Pocket PC qui permet de contrôler un pc via son PDA. Il est également possible d'utiliser les comptes Windows pour s'authentifier sur le poste distant. Enfin, tout comme VNC, il possède la fonctionnalité d'accès via un navigateur web ce qui est pratique lorsque le logiciel n'est pas implémenté sur tous les postes.

Inconvénients

PCAnywhere est un logiciel payant (199$ aux Etats-Unis pour la version boîte alors que la version Access Server coûte 399.95$ pour 25 postes) qui offre exactement les mêmes fonctionnalités que les autres produits du même genre. De plus, le serveur et le client sont relativement lourds contrairement à VNC qui occupe très peu de place sur le disque.

Bilan

PCAnywhere obtient des résultats honorables et propose des fonctionnalités plus évoluées que ses concurrents. Malgré cela, le logiciel reste payant et peut donc rebuter une bonne partie des clients potentiels.

Conclusion

Chacune des solutions d'administration à distance possède ses propres avantages ainsi que ses inconvénients. Le « Bureau à distance » de Windows est le meilleur outil dans un environnement uniquement Windows. VNC vient compléter ce dernier pour accéder aux machines UNIX. L'utilisation parallèle de ces deux logiciels vous aidera à gérer votre réseau de manière simple et efficace.

Liens

[1] Real VNC
http://www.realvnc.com/

[2] Bureau à distance
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/fr/library/ServerHelp/fb1c0f4f-3997-4659-a173-c78ff08aec1b.mspx?mfr=true

[3] PC Anywhere
http://www.symantec.com/home_homeoffice/products/overview.jsp?pcid=pf&pvid=pca12

4. ATTAQUES MAJEURES :

TOP 5 DU MOIS D'OCTOBRE

Le mois d'Octobre aura été marqué par des failles diverses pour des logiciels variés : antivirus, système d'exploitation Windows, Websphere…

10 failles Microsoft dont plusieurs jugées critiques ont été corrigées. La suite Office a été particulièrement touchée avec la découverte d'une faille affectant les trois logiciels phares : Excel, PowerPoint et Word. Parallèlement Oracle a publié son correctif trimestriel. Enfin plusieurs antivirus ont été touchés par des failles minimes.

XMCO | Partners

Microsoft

Internet Explorer et Office: toujours mauvais élèves

Dix failles ont été corrigées par Microsoft au début du mois d'Octobre.
La plus importante est une faille identifiée en Septembre. Le problème provient plus précisément du "shell" de Windows qui ne valide pas correctement les données transmises par le contrôleur ActiveX "WebViewFolderIcon". Cette vulnérabilité pouvait être exploitée par un pirate en incitant un internaute peu attentif à visiter une page Web judicieusement contrefaite. Un exploit avait été publié pour prendre le contrôle du poste vulnérable (MS06-058).

Les autres failles critiques affectent la suite Office. Chacun des composants Word, Excel et Power Point a été touchées par la même vulnérabilité.



Un correctif de type cumulatif a été publié pour ces trois logiciels qui souffraient de multiples vulnérabilités.
Un attaquant distant pouvait les exploiter afin de compromettre un système vulnérable.
La mauvaise gestion de la mémoire lors de l'ouverture de fichiers "Lotus 1-2-3" et l'utilisation d'enregistrements DATETIME, STYLE et COLINFO mal formés sont à l'origine de ces failles de sécurité. Un pirate était donc en mesure de compromettre un système impacté en exploitant ces vulnérabilités. Pour cela, il devait inciter sa victime à ouvrir un document XLS, PPT ou DOC judicieusement contrefait.

Enfin la dernière vulnérabilité critique corrigée concerne le service XML Core. Ce dernier souffrait de deux vulnérabilités. Un attaquant distant pouvait les exploiter pour compromettre un système vulnérable ou pour accéder a des informations sensibles.

La première faille vient d'une saturation de la mémoire tampon lors du traitement XSLT. Un attaquant était en mesure de compromettre un système impacté en exploitant cette vulnérabilité.

La seconde vulnérabilité résulte d'une mauvaise interprétation d'une re-direction HTTP côté serveur par le contrôle ActiveX XMLHTTP. Un attaquant pouvait alors accéder à des informations sensibles du système.
Dans les deux cas, l'exploitation des failles de sécurité nécessite l'intervention de l'utilisateur en l'invitant à visiter une page web malicieuse (MS06-061).

Les autres failles classées « Moyenne » par Microsoft concerne ASP.NET, le service serveur (déni de service), le gestionnaire de liaison et la pile TCP/IP v6. Les impacts ne sont pas élevés.

Les vulnérabilités non corrigées

Une autre faille de sécurité a été publiée quelques jours après la sortie du correctif pour PowerPoint. La vulnérabilité à été publiée par l'intermédiaire d'une preuve de concept qui a révélé l'existence d'un débordement de tampon. Le programme malicieux permet de générer un document à l'extension PPT ce qui provoque un déni de service.

De nombreux chevaux de Troie utilisent cette faille comme vecteur de diffusion. En effet, des fichiers PowerPoint contrefaits sont expédiés par courrier. Au cas où une victime ouvrirait un de ces fichiers, le téléchargement et l'installation des chevaux de Troie associés se lanceraient automatiquement.

Différents noms ont été attribués par les laboratoires d'analyse virale. Parmi ceux-ci nous pouvons identifier :

- Win32/Controlppt.W
- Exploit:Win32/Controlppt.X
- Exploit-PPT.d/Trojan.PPDropper.F

Les vecteurs d'attaques sont nombreux: envoi par e-mail, hébergement du fichier « .ppt » malicieux sur un serveur web, envoi via un logiciel de messagerie instantanée…

Quelques jours plus tard, d'autres preuves de concept ont vu le jour. Elles concernaient Internet Explorer. La première était liée à une erreur lors du traitement des objets "ADODB.Connection.Execute" malformés.
Enfin Internet Explorer 7 a été au centre de vives réactions. Deux failles, dites de spoofing, permettaient d'usurper le contenu de la barre d'adresse d' Internet Explorer 7. En incitant un internaute à visiter une page web judicieusement conçue, un pirate pourrait modifier l'URL affichée dans la barre d'adresse du navigateur. La preuve de concept publiée pouvait donc être exploitée afin de mener une attaque de Phishing.

Programmes vulnérables :
- [1] Toutes les plate-formes Windows

Criticité : Elevée
Référence Xmco
Correctif MS06-056 : 1160486983
Correctif MS06-057 : 1160486997
Correctif MS06-058 : 1160487010
Correctif MS06-059 : 1160487024
Correctif MS06-060 : 1160487045
Correctif MS06-061 : 1160487064
Correctif MS06-062 : 1160487080
Correctif MS06-063 : 1160487095
Correctif MS06-064 : 1160487095
Correctif MS06-065 : 1160487161

Antivirus

Tous vulnérables

Plusieurs antivirus ont été touchés par des failles de criticité faible. Certains exploits ont immédiatement été publiés. La plupart des failles concernent des dénis de service qui paraissent peu utiles mais qui se révèlent extrêmement efficaces.
Afin de pouvoir compromettre un système, un pirate peut s'aider de tels exploits pour désactiver les protections du système cible. L'impact de ces vulnérabilités liées aux antivirus est donc à prendre au sérieux.

McAfee

Le premier antivirus aura été Mc Afee avec la publication d'un exploit pour « Network Agent ».
Le problème résultait d'imperfections du module de traitement de certains paquets. En envoyant un paquet excessivement long sur le port 6646 à une machine utilisant le logiciel en question, le pirate pouvait provoquer l'arrêt du processus "mcnasvc.exe".

Programmes vulnérables :
- mcnasvc.exe ver1.0.178.0

Criticité : Elevée
Référence Xmco : n°1160730197

ClamAV

Le logiciel antivirus gratuit a lui aussi été la cible des chercheurs. Plusieurs vulnérabilités ont été détectées puis corrigées. Un attaquant distant était en mesure de compromettre un système vulnérable ou de causer un déni de service.
La première faille provenait de débordements de tampon du script "rebuildpe.c". Ceux-ci se manifestaient lors du traitement de certains fichiers PE malformés.
La seconde vulnérabilité résultait d'une erreur présentée au sein du script "chmunpack.c". L'exploitation de cette erreur permettait à un attaquant d'altérer le fonctionnement d'une application vulnérable.
Un programme malicieux a d'ailleurs été publié peu de temps après la découverte de cette faille. Un code "perl" générait un fichier malicieux avec l'extension « .cfm ».

Programmes vulnérables :
- Clam AntiVirus versions antérieures a 0.88.5

Criticité : Moyenne
Référence Xmco : n°1160998809/n°1161346666

Kaspersky

Le logiciel Kaspersky était également touché par une vulnérabilité due à une mauvaise gestion de la mémoire. Les pilotes "KLIN.SYS" et "KLICK.SYS" peuvent accéder à des zones de mémoires non autorisées. Ces dysfonctionnements permettent à un attaquant local d'executer des commandes arbitraires avec les privilèges "SYSTEM".

Programmes vulnérables :
- Kaspersky Anti-Virus 4.x/5.x/6.x

Criticité : Moyenne
Référence Xmco : n°1161332460

Symantec

Le leader du marché a connu plusieurs failles sur l'ensemble des produits.
Une des failles provient d'erreurs de pilotes "NAVEX15.SYS" et "NAVENG.SYS" qui ne vérifient pas correctement l'accès à certaines adresses. Ce dysfonctionnement pourrait être exploité par des attaquants locaux afin d'exécuter des commandes arbitraires avec les privilèges du noyau. [1]

Une autre vulnérabilité critique a touché les produits ePolicy Orchestrator et ProtectionPilot de McAfee. En envoyant une entête http malformée, le pirate pouvait provoquer un débordement de tampon et prendre le contrôle du poste cible. L'exploit associé a été publié et créé afin d'être utilisé par le framework Metasploit. [2]

Enfin, un autre pilote utilisé par de nombreux outils SYMANTEC permettait à un utilisateur local d'obtenir les privilèges « SYSTEM ». La faille provient d'une mauvaise validation de l'espace d'adressage mémoire au sein de la fonction "DeviceIOControl()" du pilote "SAVRT.SYS" qui permet d'écrire dans l'espace réservé au noyau du système.

Programmes vulnérables :

- [1]Norton AntiVirus
- Norton Internet Security
- Norton System Works
- Symantec AntiVirus Corporate Edition
- Symantec AntiVirus for Blue Coat Security
- Symantec AntiVirus for CacheFlow Security Gateway
- Symantec AntiVirus for Clearswift MIME Sweeper
- Symantec AntiVirus for Inktomi Traffic Edge
- Symantec AntiVirus for Microsoft ISA Server
- Symantec AntiVirus for NetApp Filer/NetCache
- Symantec BrightMail AntiSpam
- Symantec Client Security
- Symantec Mail Security for Domino
- Symantec Mail Security for Exchange
- Symantec Mail Security for SMTP
- Symantec Scan Engine
- Symantec Web Security for Windows
- [2] McAfee ePolicy Orchestrator 3.5.0 Patch 5 et versions antérieures
- McAfee ProtectionPilot 1.1.1 Patch 2 et versions antérieures
- [3] Symantec AntiVirus Corporate Edition 8.1
- Symantec AntiVirus Corporate Edition 9.0.3 et antérieures
- Symantec Client Security 1.1
- Symantec Client Security 2.0.3 et anterieures

Criticité : Elevée
Référence Xmco :
[1] N° 1160122611
[2] N° 1160146258/ N°1159784523
[3] N° 1161674285

Sophos

Plusieurs vulnérabilités ont été corrigées, au sein des Anti-Virus Sophos, qui permettaient à des attaquants distants de compromettre un système vulnérable ou de causer un déni de service.

La première faille provenait d'une erreur de type débordement de pile lors du traitement d'un fichier CHM malformé. En incitant un utilisateur à ouvrir un fichier judicieusement conçu, un attaquant pouvait exécuter des commandes arbitraires.

Le deuxième problème résultait d'une erreur, au sein du traitement d'un fichier CHM contenant une entête malformée, qui pouvait être exploitée afin d'exécuter des commandes arbitraires.

La troisième vulnérabilité provient d'une boucle infinie, lors du traitement d'une archive RAR malformée, qui pouvait être exploitée afin de causer un déni de service.

La dernière faille est liée a une erreur provoquée par le traitement d'une archive "Petite" contenant un grand nombre de secteurs. Son exploitation permettait à un attaquant d'altérer le fonctionnement de l'application vulnérable.

Programmes vulnérables :

- Adobe Flash Player 8.0.24 et antérieures
- Sophos Anti-Virus + Application Control pour Windows 2000/XP/2003 versions 6.x
- Sophos Anti-Virus pour Windows 2000/XP/2003 versions 6.x
- Sophos Endpoint Security + Application Control 2000/XP/2003 versions 6.x
- Sophos Endpoint Security versions 6.x
- Sophos Anti-Virus pour Linux (on-access) versions 5.x
- Sophos Anti-Virus pour AIX (PowerPC) versions 4.x
- Sophos Anti-Virus pour FreeBSD 6+ versions 4.x
- 5.2+ versions 4.x / 3+ versions 4.x / 4.5+ versions 4.x
- Sophos Anti-Virus pour HP-UX (AMD64, glibc 2.3) versions 4.x / (Itanium) versions 4.x
- Sophos Anti-Virus pour Linux (AMD64, glibc 2.3) versions 4.x
- Sophos Anti-Virus pour Linux (Intel, libc6) versions 4.x
- Sophos Anti-Virus pour Linux (Intel, libc6-glibc2.2) versions 4.x
- Sophos Anti-Virus pour Solaris (SPARC) versions 4.x
- Sophos Anti-Virus pour Solaris (Intel) versions 4.x
- Sophos Anti-Virus pour Tru64 UNIX (Alpha) versions 4.x
- Sophos Anti-Virus pour Windows 95/98/Me versions 4.x
- Sophos Anti-Virus pour Windows NT/2000/XP versions 4.x
- Sophos Anti-Virus pour NetWare versions 4.x
- Sophos Anti-Virus pour Windows NT versions 4.x
- Sophos Anti-Virus pour Macintosh versions 4.x
- Sophos Anti-Virus pour OS X versions 4.x

Criticité : Elevée
Référence Xmco : n°1162197578

Trendmicro

Une vulnérabilité a été identifiée dans le logiciel OfficesScan de TrendMicro. Un attaquant serait en mesure de manipuler des fichiers arbitraires en exploitant cette faille.

Le problème résulte d'une erreur au sein d'un script CGI qui ne valide pas correctement certaines requêtes HTTP. Un pirate pourrait supprimer des fichiers en forgeant des requêtes spécialement conçues.

Programmes vulnérables :

- Trend Micro OfficeScan Corporate Edition version 6.5/7.0/7.3
-

Criticité : Elevée
Référence Xmco : n°1158161811

Autres

Websphere

IBM a publié une mise à jour pour le produit IBM WebSphere Application Server versions 6.0.x. Plusieurs failles de sécurité et des bugs mineurs ont été corrigés. L'exploitation de celles-ci permettraient à un attaquant d'obtenir des informations du système cible.

La première faille résulte d'une erreur non spécifiée qui permet de visualiser le code source de certains fichiers JSP.

Le deuxième problème provient d'une erreur du dispositif de sécurité WSN qui permet d'accéder au serveur Websphere sans identifiants.

Enfin la dernière vulnérabilité résulte également d'une erreur non spécifiée dont l'impact n'a pas été déterminé.

Programmes vulnérables :

- [1] MSN, AIM et Yahoo Messenger

Criticité : Elevée

Référence Xmco : n° 1159187752 / n° 1160065984 /n° 1158921081

Oracle

Oracle a, comme tous les trois mois, publié un correctif cumulatif pour l'ensemble de ses produits (aussi bien les bases de données que dans les différents serveurs d'applications).

22 vulnérabilités sur les 95 corrigées concernent le moteur de base de données. En les exploitant, un attaquant pourrait prendre le contrôle total des bases de données.

Par ailleurs, de nombreuses vulnérabilités sont également présentes au sein du serveur HTTP (module modPL/SQL pour Apache). Ces vulnérabilités sont dangereuses car elles permettent a un attaquant distant d'exécuter des commandes arbitraires, d'accéder à des informations sensibles, d'interrompre le fonctionnement normal de l'application et de contourner les sécurités applicatives.

Plusieurs preuve de concept ont rapidement suivis la sortie du correctif. Elles permettaient à un utilisateur d'injecter des commandes SQL arbitraires et de mener des attaques de Cross Site Scripting.

Programmes vulnérables :

- Oracle Database 10g Release 2 version 10.2.0.1 et 10.2.0.2
- Oracle Database 10g Release 1 version 10.1.0.4 et 10.1.0.5
- Oracle9i Database Release 2 version 9.2.0.6 et 9.2.0.7
- Oracle8i Database Release 3 version 8.1.7.4
- Oracle Application Express (HTML DB) versions 1.5 a 2.0
- Oracle Application Server 10g Release 3 version 10.1.3.0.0
- Oracle Application Server 10g Release 2 versions 10.1.2.0.0 a 10.1.2.0.2 et 10.1.2.1.0
- Oracle Application Server 10g Release 1 (9.0.4) version 9.0.4.2 et 9.0.4.3
- Oracle Collaboration Suite 10g Release 1 version 10.1.2.0
- Oracle9i Collaboration Suite Release 2 version 9.0.4.2
- Oracle E-Business Suite Release 11i versions 11.5.7 a 11.5.10 CU2
- Oracle E-Business Suite Release 11.0
- Oracle Pharmaceutical Applications versions 4.5.0 a 4.5.1
- Oracle PeopleSoft Enterprise PeopleTools version 8.22 et 8.46 a 8.48
- Oracle PeopleSoft Enterprise Portal Solutions et Enterprise Portal version 8.8 et 8.9
- JD Edwards EnterpriseOne Tools version 8.95 et 8.96
- JD Edwards OneWorld Tools SP23
- Oracle Developer Suite versions 6i 9.0.4.1 a 9.0.4.3
- Oracle Developer Suite versions 6i 10.1.2.0.2 et 10.1.2.2
- Oracle9i Database Release 1 version 9.0.1.4, 9.0.1.5 et 9.0.1.5 FIPS
- Oracle9i Application Server Release 2 version 9.0.2.3 et 9.0.3.1
- Oracle9i Application Server Release 1 version 1.0.2.2
- Oracle Database 10g Release 1 version 10.1.0.3
- Oracle9i Database Release 2 version 9.2.0.5
- Oracle Application Server 10g Release 1 (9.0.4) version 9.0.4.1

Criticité : Urgente
Référence Xmco : n° 1161158216 / n°1161677209 / n°1161677137

5. OUTILS LIBRES :

FOCUS SUR 5 PRODUITS LIBRES

Chaque mois, nous vous présentons les outils libres qui nous paraissent indispensables. Les logiciels abordés sont variés : utilitaires de sécurité et autres programmes nécessaires au sein d'une entreprise.

Ce mois-ci, nous avons choisi d'analyser des logiciels utiles et très pratiques :

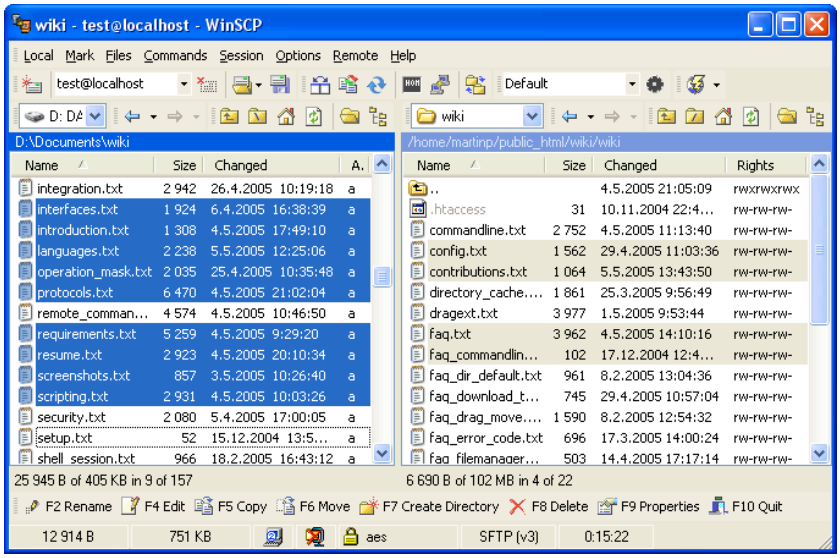
- *WinSCP : Logiciel de transfert de fichiers via le protocole SFTP*
- *Lcc : compilateur C*
- *Cain : programme de test de mots de passe*
- *RSS Bandit : agrégateur de flux RSS*
- *Netmeeting : messagerie instantanée*

Vous trouverez à la fin de cette section un tableau récapitulatif des versions de tous les logiciels présentés lors des précédents numéros d' « Actu Sécurité ».

XMCO | Partners

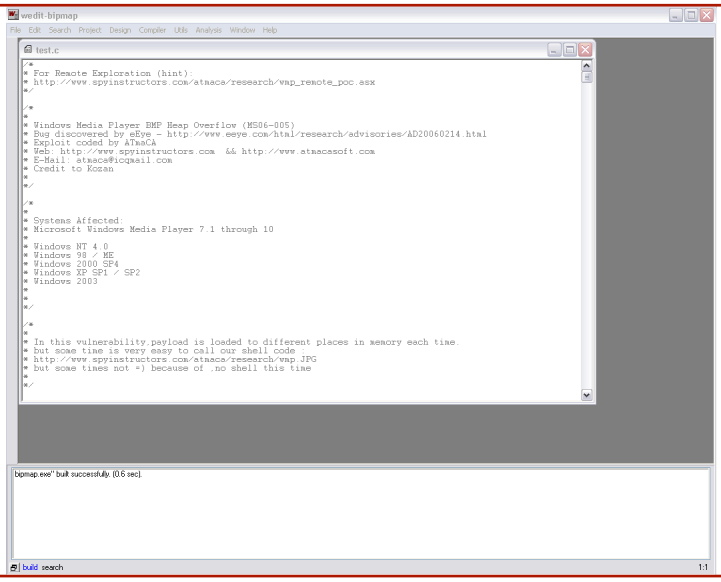
WinSCP

Client SFTP

Version actuelle	3.8.2
Utilité	★★★★☆
Type	Programme d'échange de fichiers
Description	WinSCP est un client SFTP (SSH File Transfer Protocol), basé sur SSH qui supporte les protocoles SFTP, SCP, SSH-1 et SSH-2. Il permet de copier des fichiers de manière sécurisée sur un ordinateur distant dont les machines UNIX. Il possède plusieurs fonctionnalités intéressantes : synchronisation de répertoires automatiques, création de dossiers/raccourcis sur l'ordinateur distant Ce dernier utilise un environnement graphique Windows en deux volets qui permet de glisser les fichiers locaux en toute simplicité.
Capture d'écran	
Téléchargement	WinSCP est disponible en plusieurs langues à l'adresse suivante : http://winscp.net/eng/download.php
Sécurité de l'outil	Une seule faille a été identifiée en juin 2006 et présentée dans le bulletin XMCO n°1150204443. En exploitant cette faille de sécurité un attaquant pouvait compromettre un système vulnérable.
Avis XMCO	Ce produit libre est un concurrent direct de FileZilla. Très efficace, cet outil est, cependant; moins connu et moins utilisé que le célèbre outil de Mozilla qui reste le meilleur outil dans ce domaine.

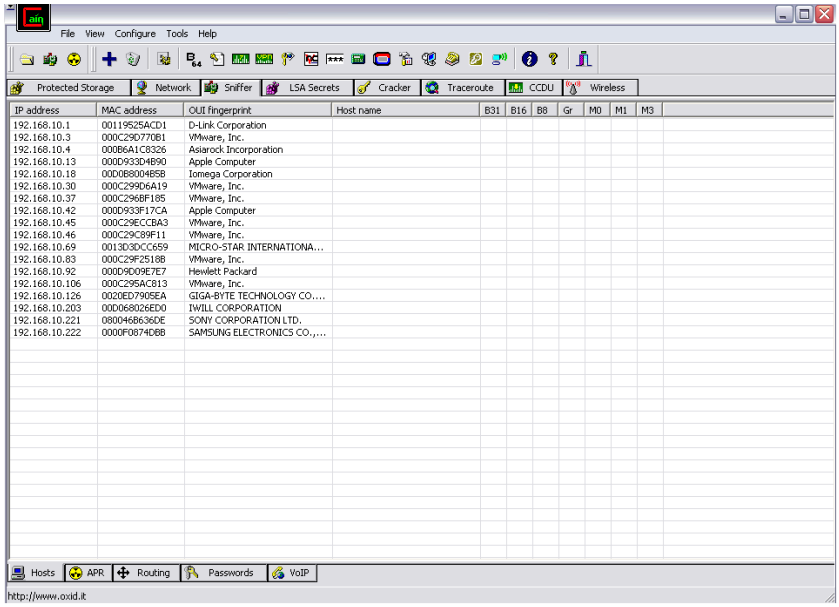
LCC

Compilateur C

Version actuelle	
Utilité	
Type	Editeur/Compilateur/Debugger C
Description	Lcc est un compilateur de language C léger et simple. Il permet de développer ou de compiler simplement les sources C ou C++. Développé par Christopher Fraser et David Hanson, Lcc est portable et adaptable sur tous les systèmes. Il se compose d'un éditeur de code (Wedit), d'un compilateur C Win32, d' un assembleur, d' un linker, d' un générateur de librairies, de plusieurs utilitaires et enfin d' un debugger intégré à Wedit. Il peut être lancé en ligne de commande mais également via l'interface graphique.
Capture d'écran	
Téléchargement	Lcc est disponible uniquement en anglais à l'adresse suivante : http://www.q-software-solutions.de/downloaders/show_download_locations
Sécurité de l'outil	Aucune faille n'a été publiée.
Avis XMCO	Ce logiciel est vraiment un outil utile et rapide pour toutes les personnes qui ont besoin de développer ou de compiler rapidement. Lcc n'utilise que très peu de ressources. Il est gratuit.

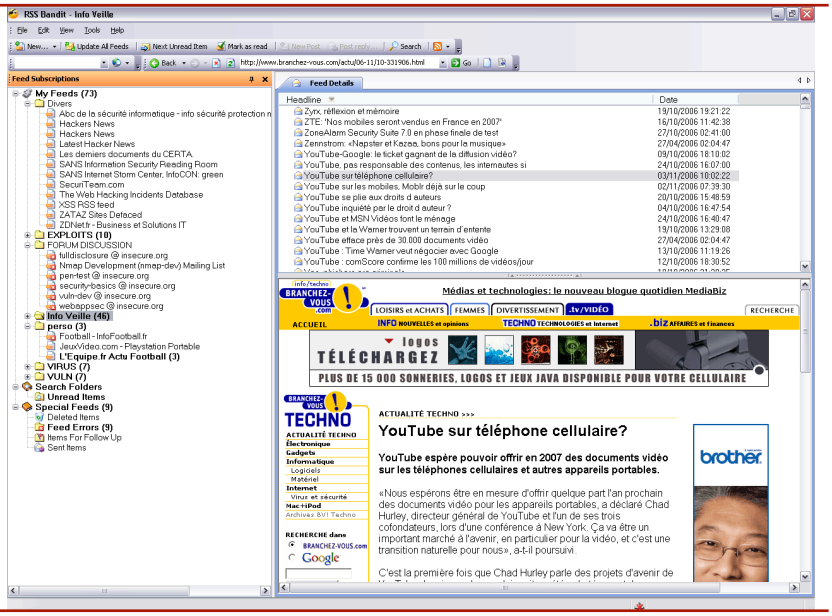
Cain

Logiciel d'audit

Version actuelle	3.3
Utilité	★★★★★
Type	Logiciel de test de mots de passe
Description	Cain et un logiciel d'audit de mot de passe pour Windows. Il permet, entre autres, de sniffer les mots de passe sur un réseau, de cracker les mots de passe chiffrés, d'enregistrer des conversations VoIP qui transitent sur le réseau ou encore de découvrir les réseaux Wifi. Cet outil est particulièrement apprécié par les administrateurs et les consultants pour tester la robustesse des mots de passe utilisés sur un réseau local.
Capture d'écran	
Téléchargement	Cain est disponible pour Windows à l'adresse suivante : http://www.oxid.it/cain.html
Sécurité de l'outil	Aucune vulnérabilité identifiée
Avis XMCO	Cain est un logiciel qui offre de nombreuses fonctionnalité intéressante : sniffing, test de mots de passe, traceroute, détection de réseaux wifi, calculateur de hash…nécessaire aux administrateurs lors de l'audit des mots de passe. Il détecte également tous les postes présents sur le même sous réseau.

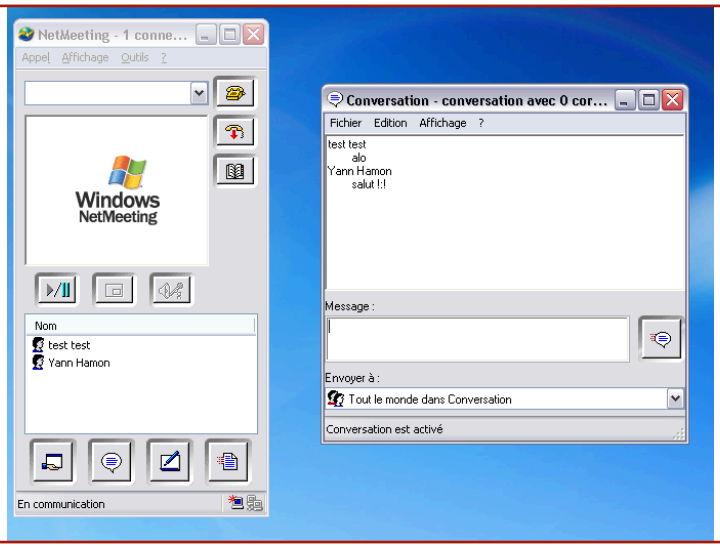
RSS Bandit

Lecteur de flux RSS

Version actuelle	3.0.42
Utilité	★★★★☆
Type	Lecteur de news et flux RSS
Description	RSS Bandit est un agégateur de flux. Il permet de rassembler de nombreux flux sur une même interface sans ralentissement. Facilement paramétrable, RSS bandit se compose de trois fenêtres principales qui rendent la lecture des news agréable et pratique. L'avantage principal réside dans la fonction « recherche » qui permet de trouver toutes les pages contenant un mot clef.
Capture d'écran	
Téléchargement	RSS Bandit est disponible à l'adresse suivante : http://www.rssbandit.org/
Sécurité de l'outil	Aucune faille n'a été publiée à ce jour.
Avis XMCO	Contrairement à Thunderbird qui propose également la fonctionnalité de flux RSS, RSS Bandit est un logiciel beaucoup plus rapide et plus intuitif. Plusieurs fonctionnalités le différencient des autres concurrents. Il est possible de sélectionner les news à lire ultérieurement. Il est capable de supporter plusieurs dizaines de flux sans aucun ralentissement notable. Sa simplicité et sa rapidité le place parmi les meilleurs outils du genre.

Netmeeting

Messagerie instantanée

Version actuelle	
Utilité	
Type	Messagerie instantanée / logiciel de visio-conférence
Description	Peu connu du grand public Netmeeting est un produit inclue sur les plates-formes Windows. Cette application réseau est un logiciel de visio-conférence qui permet également de discuter comme avec une messagerie instantanée classique. D'autres options intéressantes sont également disponibles : partage d'application (en particulier le contrôle à distance), tableau blanc, transfert de fichiers.
Capture d'écran	
Téléchargement	Netmeeting est intégré dans Windows XP et Windows serveur 2003. Il suffit d'exécuter la commande « conf » (Menu « Démarrer », « Exécuter »).
Sécurité de l'outil	Aucune faille n'a été publiée à ce jour.
Avis XMCO	Netmeeting peut être pratique pour une utilisation sur un réseau local. Aucun serveur dédié n'est nécessaire (contrairement aux messageries MSN, Yahoo messenger…). La configuration est simple, un poste doit être configuré pour recevoir la conférence et les clients viennent s'y connecter en entrant l'adresse IP du « serveur ».

Suivi des versions

Version actuelle des outils libres présentés dans les numéros précédents.

Nom	Dernière version	Date	Lien
Debian Sarge	Version stable 3.1 r2	19/04/2006	http://www.debian.org/CD/netinst/
Snort	2.6.0.2	15/09/2006	http://www.snort.org/dl/
MySQL	5.0.27		http://dev.mysql.com/downloads/mysql/5.0.html
	5.1.11-Bêta		http://dev.mysql.com/downloads/mysql/5.1.html
Apache	2.2.3		http://httpd.apache.org/download.cgi
	1.3.37		http://httpd.apache.org/download.cgi
Nmap	4.11	01/04/2005	http://www.insecure.org/nmap/download.html
Firefox	2.0	06/2006	http://www.mozilla-europe.org/fr/products/firefox/
Thunderbird	1.5.0.7	09/2006	http://www.mozilla-europe.org/fr/products/thunderbird/
Spamassassin	3.1.7	10/2006	http://spamassassin.apache.org/downloads.cgi?update=200603111700
Putty	0.58		http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
ClamAV	0.88.6	5/11/2006	http://www.clamav.net/stable.php#pagestart
Ubuntu	6.10 Edgy Eft	10/2006	http://www.ubuntu-fr.org/telechargement
Postfix	2.3	06/06/2006	ftp://ftp.club-internet.fr/pub/mirrors/ftp.porcupine.org/postfix-release/index.html
Squid	2.5	29/05/2006	http://www.squid-cache.org/Versions/v2/2.5/
Filezilla	2.2.29	1/11/2006	http://filezilla.sourceforge.net/
OpenSSH	4.4	27/09/2006	http://www.openssh.com/
Search and Destroy	1.4		http://www.safer-networking.org/fr/download/index.html
ARPWatch			ftp://ftp.ee.lbl.gov/arpwatch.tar.gz
GnuPG	1.4.5	06/2006	http://www.gnupg.org/(fr)/download/
BartPE	3.1.10a	6/10/2003	http://severinterrier.free.fr/Boot/PE-Builder/
TrueCrypt	4.2a		http://www.truecrypt.org/downloads.php

Nom	Dernière version	Date	Lien
Back-Track	2.0	10/2006	http://www.remote-exploit.org/index.php/BackTrack_Downloads
MBSA	2.0	20/08/2006	http://www.microsoft.com/technet/security/tools/mbsahome.mspx
Ps-Exec	1.7		http://www.sysinternal.com/Utilities/PsExec.html
Helios	v1.1a	6/10/2003	http://helios.miel-labs.com/2006/07/download-helios.html
Opera	9.02		http://www.opera.com/download/
Internet Explorer 7	Internet Explorer 7		http://www.microsoft.com/windows/ie/downloads/default.mpsx
Outil de suppression de logiciels malveillants	1.21	10/10/2006	http://www.microsoft.com/downloads/details.aspx?FamilyID=ad724ae0-e72d-4f54-9ab3-75b8eb148356&DisplayLang=fr
F-Secure Blacklight	Blacklight Beta		http://www.f-secure.com/blacklight/try_blacklight.html
Writely	Writely beta		http://www.writely.com
Nessus	3.0.3		http://www.nessus.org/download
Windows Services for Unix	3.5		http://www.microsoft.com/france/windows/sfu/decouvrez/detail.mspx
VNC	4.2.7		http://www.realvnc.com/cgi-bin/download.cgi
Vmware Player	1.0.2		http://www.vmware.com/download/player/
Sync Toy	1.4		http://www.microsoft.com/downloads/details.aspx?FamilyID=E0FC1154-C975-4814-9649-CCE41AF06EB7&displaylang=en
MySQL Front	3.0		http://www.clubic.com/lancer-le-telechargement-9175-0-mysql-front.html