Windows XP Service Pack 2 : point de vue du développeur
Version préliminaire pour la PDC 2003

Ce document contient des informations préliminaires sur les technologies de sécurité intégrées dans Windows XP SP2.

Microsoft Corporation

Octobre 2003

Concerne :

Microsoft® Windows® XP

Résumé : Avec Windows XP Service Pack 2 (SP2), Microsoft introduit un ensemble de technologies de sécurité qui améliorent la protection des ordinateurs sous Windows XP contre les attaques de virus. Ces technologies incluent notamment :

- Protection du réseau
- Protection de la mémoire
- Amélioration de la sécurité du courrier électronique
- Amélioration de la navigation sur le Web

Ce document porte sur les deux premières technologies.

Ce document décrit certaines spécificités du SP2 et leurs implications pour les développeurs. D'autres informations seront régulièrement proposées à l'intention des développeurs sur le site Web MSDN US et MSDN Français. L'objectif du SP2 est de continuer les efforts de l'initiative Trustworthy Computing (vers une informatique de confiance) déjà appliqués dans Windows Server 2003. Pour en savoir plus sur l'initiative Microsoft Trustworthy Computing, consultez le document Trustworthy Computing Defined. (13 pages).

Présentation des technologies de sécurité de Windows XP SP2

De nombreux clients n'appliquent pas immédiatement tous les correctifs disponibles mais doivent néanmoins être protégés vis-à-vis des menaces endiguées par ces correctifs. Chaque bulletin de sécurité proposé par Microsoft fournit des informations permettant aux clients d'atténuer les risques tout en déployant le correctif. Microsoft va maintenant plus loin avec des technologies de sécurité en offrant une protection supplémentaire avant le déploiement d'un correctif. Ces technologies concernent les aspects suivants :

- **Protection du réseau.** Ces technologies de sécurité offrent une meilleure protection contre les attaques réseau de type Blaster grâce à de nombreuses améliorations, notamment celle du pare-feu de connexion Internet (ICF). Il est ainsi prévu d'activer ICF par défaut dans les installations du SP2, de fermer les ports inutilisés, d'améliorer l'interface utilisateur pour la configuration, d'accroître la compatibilité des applications lorsque ICF est activé et de simplifier l'administration d'ICF en entreprise grâce à une stratégie de groupe. La surface d'attaque du service RPC sera réduite et son privilège d'exécution restreint. L'infrastructure DCOM sera dotée de restrictions de contrôle d'accès supplémentaires pour réduire les risques d'attaque réseau.

- **Protection de la mémoire.** Certaines attaques exploitent des vulnérabilités logicielles permettant la copie d'une grande quantité de données dans certaines zones de la mémoire de l'ordinateur. Ces vulnérabilités sont généralement qualifiées de saturations de mémoire tampon (*buffer overruns*). Bien qu'aucune technologie spécifique ne puisse éliminer ce type de vulnérabilité, Microsoft emploie un certain nombre de techniques pour contrer ces attaques. D'abord, certains composants principaux de Windows sont recompilés avec la version la plus récente de notre compilateur pour atténuer les risques de saturation de mémoire tampon. Microsoft travaille également en collaboration étroite avec les constructeurs de microprocesseurs pour intégrer dans Windows la prise en charge de la sécurité matérielle « no execute » (ou NX) sur les microprocesseurs dotés de cette fonction. Cette approche utilise le processeur lui-même pour réaliser la séparation entre le code de l'application et les données, empêchant ainsi une application ou un composant Windows d'exécuter un code qu'un ver ou un virus aurait inséré dans une partie de la mémoire réservée aux données.

- **Amélioration de la sécurité du courrier électronique.** Des technologies de sécurité contribueront à stopper les virus (tels que SoBig.F) diffusés par courrier électronique et messagerie instantanée. Elles incluent des paramètres par défaut plus sécurisés, un contrôle amélioré des pièces jointes pour Outlook Express et Windows Messenger, une meilleure sécurité et une plus grande fiabilité d'Outlook Express. Les pièces jointes potentiellement dangereuses envoyées par courrier électronique et dans des messages instantanés seront isolées afin de ne pas corrompre d'autres parties du système.

- **Amélioration de la navigation sur le Web.** Les technologies de sécurité incorporées dans Internet Explorer assureront une meilleure protection contre le contenu malveillant sur le Web. L'une de ces améliorations prévoit le verrouillage de la zone Machine locale pour empêcher l'exécution de scripts malveillants et renforcer la protection contre les téléchargements Web hostiles. Nous fournirons également des contrôles et des interfaces utilisateur améliorés qui interdiront l'exécution sournoise de contrôles ActiveX® malveillants et de logiciels espions sans que l'utilisateur ne le sache ni ne l'ait acceptée.

Microsoft reconnaît que ces technologies de sécurité ne constituent qu'un aspect d'une stratégie de sécurité globale et approfondie.

Protection du réseau dans Windows XP SP2

Dans Windows XP SP2, Microsoft a développé trois technologies clés pour rendre les systèmes moins vulnérables aux attaques sur le réseau :

- **Pare-feu de connexion Internet.** Le pare-feu de connexion Internet (ICF) fonctionne par filtrage de paquets avec état. Il est inclus dans Windows XP et Windows Server 2003. ICF assure la protection des PC connectés à un réseau en interdisant les connexions entrantes non sollicitées du protocole TCP/IP version 4 (IPv4). Le SP2 active ICF par défaut et le démarre plus tôt dans le processus d'amorçage.

- **Restriction de l'interface RPC.** La restriction de l'interface (exposée aux développeurs, par exemple, au moyen de la nouvelle clé de registre **RestrictRemoteClients**) modifie le comportement de toutes les interfaces d'appel de procédures à distance sur le système et, par défaut, élimine l'accès anonyme à distance aux interfaces RPC, à quelques exceptions près. En pratique, la restriction de l'interface RPC oblige les appelants à s'authentifier, ce qui complique singulièrement l'attaque d'une interface. Cette mesure est particulièrement utile contre les chevaux de Troie qui ont tendance à s'appuyer sur des saturations de mémoire tampon pouvant être invoquées à distance par le biais de connexions anonymes.

- **Modifications de DCOM.** Le SP2 apporte deux modifications au comportement du modèle DCOM (Distributed Component Object Model). Il introduit d'abord au niveau de l'ordinateur des restrictions globales qui assurent un contrôle d'accès supplémentaire à partir d'une ACL globale (liste de contrôle d'accès) lors de chaque appel, activation ou lancement d'un serveur COM sur l'ordinateur. Deuxièmement, il introduit un ensemble d'autorisations COM plus précis, permettant aux administrateurs de contrôler avec souplesse la stratégie des autorisations COM d'un ordinateur.

Remarque Si vous utilisez COM uniquement pour des composants COM in-process, le SP2 n'aura pas d'incidence sur votre application.

Pare-feu de connexion Internet dans Windows XP SP2

Dans le SP2, ICF inclut une multitude de nouvelles fonctions. Ce document en décrit cinq qui auront un effet sur les applications existantes :

1. **Activé par défaut.** Avant le SP2, ICF était désactivé par défaut dans Windows XP ; les utilisateurs devaient exécuter un Assistant ou accéder au dossier Connexions réseau pour activer ICF. L'activation par

défaut d'ICF protégera l'ordinateur contre de nombreuses attaques réseau. Par exemple, si ICF avait été activé par défaut, l'impact de la récente attaque Blaster aurait été considérablement réduit, quels que soient les correctifs installés. Cette modification peut avoir un impact sur les applications existantes si ces applications utilisent des ports ou des protocoles bloqués par défaut par ICF.

2. **Sécurité pendant le démarrage.** Dans les versions précédentes de Windows, il existait un intervalle de temps entre le démarrage de la pile réseau et la mise en place de la protection ICF. Par conséquent, un paquet pouvait être reçu et livré à un service sans être filtré par ICF, créant ainsi une vulnérabilité. Dans le SP2, le pilote du pare-feu a une règle statique nommée stratégie de démarrage prévoyant l'exécution d'un filtrage pendant la mise en place du système d'exploitation. Cela permet à l'ordinateur d'effectuer des tâches réseau de base telles que DNS et DHCP et de communiquer avec un contrôleur de domaine pour obtenir une stratégie. Une fois le service de pare-feu totalement chargé et actif, il applique la stratégie ICF et retire le filtre de démarrage. Cette modification devrait améliorer la sécurité du système sans incidence sur les applications.

3. **Liste blanche d'applications.** Avant le SP2, les applications devaient appeler les API ICF pour activer les ports à ouvrir afin d'envoyer et de recevoir des messages. Cette technique s'est avérée difficile à mettre en œuvre dans des situations de connexion point à point lorsque le port n'était pas connu d'avance. Il revenait en outre à l'application de fermer l'ouverture du pare-feu, ce qui pouvait entraîner des ports restant ouverts dans le pare-feu si l'application se terminait accidentellement. En outre, ces ouvertures ne pouvaient être effectuées que par des applications fonctionnant dans le contexte de sécurité d'un administrateur local. Dans le SP2, une application qui doit écouter le réseau peut être ajoutée à la liste des applications autorisées (liste blanche). Pour une application figurant dans la liste blanche, l'ouverture des ports en écoute est effectuée automatiquement. Lorsqu'une application figure sur la liste blanche, seuls les ports nécessaires sont ouverts et uniquement tant que l'application reste à l'écoute. Cela empêche une application d'ouvrir un port qu'elle n'utilise pas et d'exposer délibérément ou non une autre application ou un autre service au trafic réseau à partir de ce port. Cela permet également aux applications écoutant le réseau de s'exécuter sous l'identité d'un utilisateur habituel, sans avoir besoin des droits d'administrateur. Les applications compatibles avec le filtrage d'ICF n'ont pas besoin de figurer sur la liste blanche. Les administrateurs sont seuls habilités à ajouter une application à cette liste.

4. **Support RPC.** Dans les versions antérieures de Windows, ICF bloquait la communication RPC, entraînant la défaillance de certaines fonctions, telles que le partage de fichiers et d'imprimantes et l'administration à distance. Cet incident se produisait parce que le nom du fichier du processus RPC était le même pour de nombreux serveurs RPC (svchost.exe). Le SP2 permet un contrôle précis des services RPC ayant la possibilité de traverser ICF. Lors de l'ouverture d'un port, un appelant peut demander l'utilisation de ce port pour RPC. ICF n'accepte cette demande que si l'appelant fonctionne dans les contextes de sécurité Système local, Service réseau ou Service local. ICF prend en charge un indicateur du niveau de profil qui permet d'ouvrir des ports RPC même si l'appelant ne figure pas sur la liste blanche des applications : **PrivilegedRpcServerPermission**. Avec cette granularité, les administrateurs peuvent contrôler les services RPC exposés au réseau, limitant la communication à ceux qui en ont besoin.

5. **Mode « blindé ».** Si une application malveillante qui trouve et exploite une vulnérabilité dans l'un des services à l'écoute dans Windows constitue une menace pour les utilisateurs, le SP2 comporte un nouveau paramètre pour ICF, le mode « shielded (blindé) ». Ce mode permet aux utilisateurs de se protéger facilement en paramétrant ICF de façon à empêcher tout trafic entrant non sollicité jusqu'à ce qu'un correctif soit disponible, sans devoir reconfigurer le pare-feu. Dans ce mode, l'ordinateur ne peut pas écouter les requêtes qui proviennent du réseau. Les connexions sortantes sont les seules autorisées. Un appel API cherchant à effectuer une ouverture statique sera autorisé et la configuration enregistrée, mais il ne sera pas appliqué tant que le mode opérationnel d'ICF ne sera pas revenu à la normale.

Implications pour les développeurs

Pour de nombreuses applications, aucune modification ne sera nécessaire. La navigation sur le Web, la vérification du courrier électronique et la messagerie instantanée fonctionneront avec les modifications d'ICF apportées dans le SP2. Cependant, dans certains cas, les développeurs voudront tirer parti des nouvelles fonctionnalités d'ICF ou changer leurs applications de telle façon qu'elles fonctionnent correctement lorsque ICF est activé par défaut.

- **Connexions IPv4 entrantes pour les applications.** Une application qui exécute une opération d'écoute sur un socket TCP ou se lie à un socket UDP par l'intermédiaire de Winsock est couverte par ce scénario. Des exemples de ces applications comprennent notamment des séquences audio et vidéo dans MSN ou Windows Messenger, ou l'hébergement d'un jeu à plusieurs participants. Pour ce scénario, ICF peut automatiquement ouvrir et fermer les ports requis par l'application. Lorsqu'une application devant écouter un ou des ports est installée par un administrateur, celui-ci devra demander à l'utilisateur s'il souhaite permettre à l'application d'ouvrir des ports dans le pare-feu. Si l'utilisateur accepte, l'application doit utiliser l'API INetFwV4AuthorizedApplication pour s'ajouter à la collection AuthorizedApplications

comme application activée. Si l'utilisateur refuse, l'application doit utiliser l'API INetFwV4AuthorizedApplication pour s'ajouter à la collection AuthorizedApplications comme application désactivée.

- **Connexions entrantes IPv4 pour les services.** Dans des scénarios tels que le partage de fichiers et d'imprimantes et le partage de bureau à distance, où Windows XP doit accepter une connexion entrante à un service, les développeurs auront à modifier certaines parties du code. Bien que les développeurs soient invités à utiliser les API AuthorizedApplication pour tous les autres scénarios, l'utilisation des API de port global d'ICF est conseillée pour les services qui écoutent des ports fixes. Ces ports étant toujours ouverts, leur ouverture dynamique n'offrirait que peu d'avantages. En revanche, les utilisateurs ont la possibilité de personnaliser les paramètres du pare-feu pour ces ports fixes lorsque les API de port global sont utilisées. Lorsqu'un service doit écouter un port fixe, il doit demander à l'utilisateur s'il souhaite permettre au service d'ouvrir des ports dans le pare-feu. Si l'utilisateur accepte, le service doit utiliser l'API INetFwV4OpenPort pour ajouter des règles à ICF afin d'ouvrir le ou les ports fixes dont il a besoin. Ces règles doivent être activées. Si l'utilisateur refuse, le service doit quand même utiliser l'API INetFwV4OpenPort pour ajouter des règles à ICF afin d'ouvrir le ou les ports fixes dont il a besoin mais ces règles ne seront pas activées.

- **Connexions IPv4 entrantes sur des ports RPC et DCOM.** Certaines applications et certains services nécessitent l'utilisation de ports RPC, par DCOM ou directement par RPC pour les connexions entrantes. En raison des implications significatives sur la sécurité lors de l'ouverture de ports RPC, ces ports doivent être gérés comme un cas particulier et les développeurs ne devraient tenter d'activer RPC via ICF que lorsque cela est absolument nécessaire. ICF inclut un paramètre explicite dans le pare-feu autorisant l'ouverture et la fermeture automatique de ports pour RPC. Par conséquent, les applications et les services n'ont pas besoin d'ouvrir des ports spécifiques pour utiliser RPC pour des connexions entrantes. Cependant, RPC sera bloqué par défaut par ICF. Cela signifie qu'une application ou un service devrait autoriser les ports RPC dans ICF. Si les ports RPC sont déjà autorisés, l'application ou le service fonctionne correctement sans rien faire. Si l'utilisateur accepte d'autoriser les ports RPC, l'application ou le service doit employer l'API INetFwV4Profile pour attribuer la valeur True à **AllowRpcPorts** afin de permettre un trafic sur ces ports. Si l'utilisateur refuse d'autoriser les ports RPC, l'application ou le service ne doit pas configurer ICF pour autoriser les ports RPC.

Restriction de l'interface RPC

Lorsqu'une authentification est imposée aux appels, même s'il s'agit d'un niveau d'authentification relativement faible, il devient beaucoup plus difficile d'attaquer une interface RPC.

Avec le SP2, Microsoft apporte un certain nombre de modifications à l'infrastructure RPC rendant les interfaces RPC plus sécurisées par défaut et réduisant la surface d'attaque de Windows XP. Le changement le plus significatif est l'ajout de la clé de registre **RestrictRemoteClients**. Cette clé modifie le comportement de toutes les interfaces RPC du système et élimine, par défaut, l'accès anonyme à distance aux interfaces RPC sur le système, à quelques exceptions près.

- **RestrictRemoteClients.** Lorsqu'une interface est enregistrée par l'intermédiaire de **RpcServerRegisterIf***, RPC permet à l'application serveur de restreindre l'accès à l'interface, généralement au moyen d'une fonction de rappel de sécurité. La clé de registre **RestrictRemoteClients** oblige RPC à effectuer des contrôles de sécurité supplémentaires pour toutes les interfaces, même si la fonction de rappel de sécurité n'est pas enregistrée pour l'interface. Si votre application RPC s'attend à recevoir des appels provenant de clients RPC anonymes, ce changement risque d'avoir un impact sur votre application. Trois options permettent de garantir que votre application continue à fonctionner normalement :

    - Vous pouvez demander à vos clients RPC d'utiliser la sécurité RPC lorsqu'ils contactent votre application serveur. C'est la meilleure méthode pour atténuer les menaces à la sécurité.

    - Vous pouvez exempter votre interface en fournissant **RPC_IF_ALLOW_CALLBACKS_WITH_NO_AUTH** pendant l'enregistrement de l'interface. Cette valeur configure RPC pour permettre des connexions anonymes uniquement sur cette interface.

    - Vous pouvez définir la clé de registre à **RPC_RESTRICT_REMOTE_CLIENT_NONE (0)** pour forcer RPC à adopter le même comportement que dans les versions précédentes de Windows.

- **EnableAuthEpResolution.** Cette clé permet d'activer le scénario **RestrictRemoteClients** décrit dans la section précédente. Lorsque cette clé est activée, toutes les requêtes du mappeur de point de connection RPC exécutées au nom d'appels authentifiés seront effectuées en utilisant l'authentification NTLM. Cela permet à un client RPC d'effectuer un appel à un serveur RPC qui a enregistré un point de terminaison

dynamique sur un système SP2. L'ordinateur client doit définir cette clé de registre afin de pouvoir effectuer une requête au mappeur de point de connection RPC authentifié. Une interface RPC accessible à distance et de façon anonyme et qui est enregistrée par défaut sur Windows XP présente une vulnérabilité. RPC lui-même doit enregistrer une telle interface pour assurer une résolution de point de connection pour des appels en utilisant des points de terminaison dynamiques. Avec l'ajout de l'indicateur **RestrictRemoteClients**, l'interface du mappeur de point de connection RPC ne sera plus accessible de façon anonyme par défaut. Cette mesure améliore sensiblement la sécurité mais modifie la tâche de résolution d'un point de connection. Actuellement, un client RPC qui tente d'effectuer un appel en utilisant un point de connection dynamique interroge d'abord le mappeur de point de connection sur l'ordinateur serveur pour déterminer à quel point de connection il doit se connecter. Cette requête est effectuée de façon anonyme même si l'appel du client RPC est lui-même exécuté en utilisant la sécurité RPC. Les appels anonymes à l'interface du mappeur de point de connection échoueront par défaut sur Windows XP SP2 en raison de la valeur par défaut de la nouvelle clé **RestrictRemoteClients**. Il est donc nécessaire de changer le module client RPC de manière à effectuer une requête authentifiée au mappeur de point de connection. Si la clé **EnableAuthEpResolution** est activée, le module client RPC utilisera NTLM pour s'authentifier au mappeur de point de connection. Cette requête authentifiée se produira uniquement si l'appel au client RPC est effectué en utilisant l'authentification RPC.

Modifications apportées à DCOM

Le SP2 apporte deux modifications au comportement du modèle DCOM (Distributed Component Object Model) : les restrictions à l'échelle de l'ordinateur et les autorisations COM granulaires. Si vous utilisez COM pour les composants COM in-process, le SP2 n'aura pas d'incidence sur votre application.

Restrictions à l'échelle de l'ordinateur

Les restrictions à l'échelle de l'ordinateur fournissent un contrôle d'accès supplémentaire via une ACL (liste de contrôle d'accès) définie au niveau de l'ordinateur. Ce contrôle a lieu lors de chaque appel, activation ou lancement d'un serveur COM sur l'ordinateur. Si la fonction AccessCheck échoue, la requête d'appel, d'activation ou de lancement est refusée.

Ces restrictions atténuent les risques liés aux paramètres trop permissifs utilisés par de nombreuses applications COM. Elles fournissent aux administrateurs un niveau plus élevé de connaissance et de contrôle des paramètres de sécurité sur toutes les applications COM enregistrées sur un ordinateur. Elles offrent également à l'administrateur la possibilité de désactiver une activation, un lancement et des appels DCOM entrants. Ces contrôles d'accès sont comparables à un AccessCheck effectué sur une ACL lors de chaque appel, chaque activation ou chaque lancement d'un serveur DCOM sur l'ordinateur. Si la fonction AccessCheck échoue, la requête d'appel, d'activation ou de lancement est refusée. Ce contrôle vient compléter toute fonction AccessCheck pouvant être exécutée sur les ACL spécifiques du serveur. En effet, il constitue une barrière d'autorisation minimale qui doit être franchie pour accéder aux serveurs COM. Il y aura dorénavant une liste ACL à l'échelle de l'ordinateur pour les autorisations de lancement (pour traiter l'activation et le lancement) et une liste ACL à l'échelle de l'ordinateur pour les autorisations d'accès (pour traiter les appels). Ces listes peuvent être configurées par l'intermédiaire du composant logiciel enfichable MMC Services des composants.

Implications pour les développeurs

Ces changements risquent d'avoir des incidences sur certaines applications. Notamment, si l'application prévoit par défaut que tout utilisateur se voit accorder les autorisations d'appel à distance, le SP2 désactive par défaut les scénarios qui impliquent des appels à distance non authentifiés. Le SP2 devrait autoriser la plupart des

scénarios client DCOM, notamment le cas le plus fréquent dans lequel un client DCOM passe une référence locale à un serveur distant, transformant ainsi le client en serveur DCOM. Le SP2 devrait autoriser le déroulement de tous les scénarios locaux sans modification du logiciel ou du système d'exploitation.

Si vous mettez en place un serveur DCOM et prévoyez de prendre en charge une activation à distance par un client DCOM non administratif, vous devriez vous demander si cette configuration est la meilleure. Si vous pensez que c'est le cas, vous devrez changer la configuration par défaut de cette fonction. Si vous mettez en place un serveur DCOM et prévoyez de prendre en charge les appels non authentifiés à distance, vous devriez vous demander si cette configuration est la meilleure. Si vous pensez que c'est le cas, vous devrez changer la configuration par défaut de cette fonction.

Autorisations COM granulaires

Les autorisations DCOM granulaires offrent aux administrateurs une grande souplesse de contrôle sur la stratégie des autorisations DCOM d'un ordinateur reposant sur le concept de « distance ». Dans les systèmes Windows XP existants, lorsque des utilisateurs ont accès à serveur DCOM, cet accès s'applique à une utilisation locale et distante. L'application du serveur DCOM n'a aucun moyen de fournir un contrôle plus précis. Le SP2 introduit les autorisations DCOM granulaires, qui offrent aux utilisateurs la souplesse de contrôler la stratégie d'autorisation DCOM d'un ordinateur en fonction du concept de « distance ». Le SP2 définit deux distances : accès *local* et accès *distant*. Un message COM local arrive par l'intermédiaire du protocole LRPC, tandis qu'un message COM distant arrive par l'intermédiaire d'un protocole tel que TCP. La possibilité de détecter qu'un appel RPC provient d'une source distante, et donc peut-être potentiellement dangereux, atténue les risques d'attaques par le réseau.

Le SP2 change également COM de manière à séparer les autorisations d'appel et d'activation, et à déplacer les autorisations d'activation, de l'ACL des autorisations d'accès vers l'ACL des autorisations de lancement. Il est ainsi possible de prendre en charge les serveurs DCOM qui nécessitent un accès non authentifié pour gérer les rappels, tout en limitant qui peut acquérir une référence d'objet initial en restreignant les droits d'activation. Plutôt que de distinguer uniquement le local du distant, nous séparerons les accès en quatre droits : lancement local (LL « Local Launch »), lancement à distance (RL « Remote Launch »), activation locale (LA « Local Activation ») et activation à distance (RA « Remote Activation »). Nous pensons assurer ainsi une compatibilité maximale, tout en limitant les activations à distance afin d'administrer et fournir un modèle souple et cohérent. Ainsi, il est possible de configurer le système pour autoriser les appels anonymes tout en continuant à contrôler l'activation. L'activation et le lancement étant tous deux liés à l'acquisition d'un pointeur d'interface, les droits d'accès à l'activation et au lancement appartiennent logiquement à une seule et même ACL. En outre, puisque les autorisations de lancement sont toujours spécifiées par une configuration mettant en jeu des autorisations d'accès, lesquelles sont souvent spécifiées par programme, l'ajout de l'autorisation d'activation dans l'ACL des autorisations de lancement permet à l'administrateur de contrôler l'activation.

Pour garantir la compatibilité, les descripteurs de sécurité DCOM existants seront interprétés de façon à autoriser ou à refuser simultanément l'accès local et distant. Ainsi, une ACE (entrée de contrôle d'accès)

autorisera les accès locaux et distants, ou les refusera.

Il n'y a aucun problème de compatibilité ascendante pour les droits d'appel ou de lancement. Il y a toutefois un problème de compatibilité pour les droits d'activation. Si, dans les descripteurs de sécurité existants pour un serveur DCOM, les autorisations de lancement configurées sont plus restrictives que les autorisations d'accès, et sont plus restrictives que les conditions minimales imposées pour les scénarios d'activation client, l'ACL des autorisations de lancement devra être modifiée pour autoriser les clients habilités.

Pour les applications DCOM qui utilisent les paramètres de sécurité par défaut, il n'y a aucun problème de compatibilité. Pour les applications qui sont démarrées dynamiquement par l'intermédiaire d'une activation DCOM, la plupart ne présentent aucun problème de compatibilité puisque les autorisations de lancement doivent déjà inclure quiconque a la possibilité d'activer un objet. Si ces autorisations ne sont pas correctement configurées, des échecs d'activation risquent de se produire si des appelants sans autorisation de lancement essaient d'activer un objet lorsque le serveur n'est pas déjà en service.

Implications pour les développeurs

Les applications les plus susceptibles de présenter des problèmes de compatibilité sont les applications DCOM qui sont déjà démarrées par l'intermédiaire d'un autre mécanisme (par exemple l'interpréteur de commandes, le gestionnaire de contrôle des services). Ces applications pourraient également être démarrées par l'intermédiaire d'une activation DCOM précédente qui a préséance sur les autorisations d'accès et de lancement par défaut et qui spécifie des autorisations de lancement qui sont plus restrictives que les autorisations d'appel. Vous trouverez ci-dessous des informations détaillées sur les solutions à apporter à ce problème de compatibilité.

Si un système qui a été mis à jour avec Windows XP SP2 est restauré à un niveau de Service Pack antérieur, toute ACE qui a été modifiée pour autoriser un accès local, un accès distant, ou les deux, sera interprétée de façon à autoriser l'accès local et distant. Toute ACE qui a été modifiée pour refuser un accès local, un accès distant, ou les deux, sera interprétée de façon à refuser l'accès local et distant. Vous devez vous assurer que toutes les ACE sont vérifiées lors de la désinstallation d'un Service Pack.

Si vous mettez en place un serveur DCOM et remplacez les paramètres de sécurité par défaut, vérifiez que l'ACL des autorisations de lancement propre à l'application accorde une autorisation d'activation aux utilisateurs appropriés. Dans le cas contraire, vous devrez changer votre autorisation de lancement spécifique de l'application afin d'attribuer des droits d'activation aux utilisateurs appropriés. Ces autorisations de lancement spécifiques de l'application sont enregistrées dans le registre.

Les listes ACL DCOM peuvent être créées ou modifiées au moyen de fonctions de sécurité normales. Pour plus d'informations, reportez-vous au document Using Access Control dans MSDN.

Protection de la mémoire dans Windows XP SP2

Cette section décrit le principal type de protection de niveau système que Microsoft met en œuvre dans le SP2 :

- **Protection d'exécution (no execute ou NX).** NX fait appel à des fonctions du processeur pour marquer la mémoire afin que le code ne puisse pas être exécuté à partir de cette mémoire, limitant ainsi les risques d'attaques par des vers de type Blaster.

NX compliquera singulièrement l'exploitation malveillante (ou même accidentelle) de saturations des mémoires tampons dans Windows XP SP2. Le SP2 pourrait également inclure d'autres protections de niveau système ; nous diffuserons des informations à ce sujet sur le site MSDN Security Developer Center dès qu'elles seront disponibles.

Protection d'exécution

La protection d'exécution (NX, no execute) est une fonction du système d'exploitation qui repose sur les caractéristiques matérielles du processeur. Elle marque la mémoire avec un attribut indiquant qu'un code ne peut pas être exécuté à partir de cette mémoire. La protection d'exécution est mise en œuvre au niveau des pages de mémoire virtuelle, utilisant le plus souvent un bit dans la table des pages (PTE) pour marquer chaque page.

La protection d'exécution empêche l'exécution d'un code à partir de pages de données, telles que le tas (*heap)* par défaut, diverses piles et des pools de mémoire. La protection peut être appliquée en mode utilisateur ou en mode noyau. Comme la protection d'exécution empêche l'exécution de données à partir de la pile, l'action spécifique effectuée par le récent ver Blaster aurait entraîné une violation d'accès mémoire et la fin du processus. Sur un système doté de la protection d'exécution, Blaster aurait été limité à une attaque de type déni de service et n'aurait pas eu la possibilité de se répliquer et de se répandre sur d'autres systèmes. Cette protection aurait atténué de façon significative la portée et l'impact du ver. Bien que Blaster sous sa forme d'origine ne fasse pas partie des pires menaces, la protection d'exécution constitue une défense complète contre tous les virus, vers et autres codes malveillants.

La mise en œuvre matérielle de cette protection et le marquage de la page de mémoire virtuelle varient en fonction de l'architecture du processeur. Cependant, les processeurs prenant en charge la protection d'exécution peuvent générer une exception lorsqu'un code est exécuté à partir d'une page marquée avec l'activation d'un attribut particulier. La version 32 bits de Windows utilise actuellement la fonction de processeur NX, telle que définie dans le manuel du programmeur de l'architecture AMD64. Pour exploiter cette fonction de processeur, le processeur doit fonctionner en mode PAE (Physical Address Extension).

Bien que les seules familles de processeurs actuellement commercialisées et offrant la prise en charge matérielle compatible Windows pour la protection d'exécution sont l'AMD K8 et la famille de processeurs Intel Itanium, il est prévu que d'autres processeurs 32 et 64 bits offrent rapidement cette protection. Microsoft encourage cette tendance en prenant en charge cette protection dans ses systèmes d'exploitation de pointe.

Microsoft prendra en charge les nouveaux processeurs dotés de la protection d'exécution en faisant évoluer Windows, à partir du SP2. Cette protection offre des avantages évidents contre les attaques par saturations de

mémoires tampons et favorise l'adoption de pratiques de programmation rigoureuses chez Microsoft et les développeurs tiers. Le tableau 1 ci-dessous présente les divers types de zones de mémoire en mode utilisateur et leur protection d'exécution par défaut.

Tableau 1. Protection d'exécution en mode utilisateur (système d'exploitation 32 bits)

Type de zone de mémoire	La zone est-elle exécutable ?	
	SP2	Windows XP
Protection d'exécution activée à l'échelle du système ?	Oui	Non
Pile	Non	Oui
Segment de mémoire (tas)	Par défaut, non	Oui

Implications pour les développeurs

Certains comportements d'application risquent d'être incompatibles avec la protection d'exécution. Par exemple, les applications qui effectuent une génération de code dynamique (telle que la génération de code Juste-à-temps) et qui ne marquent pas explicitement le code généré avec une autorisation d'exécution risquent de présenter des problèmes de compatibilité avec la protection d'exécution. Notez que les applications à code géré et les composants reposant sur la CLR (Common Language Runtime) de .NET Framework continueront à fonctionner, la CLR étant compatible avec la protection d'exécution dans Windows XP SP2.

Les développeurs d'applications et de pilotes doivent tenir compte de la protection d'exécution et des exigences du logiciel utilisé sur une plate-forme compatible. Les applications qui génèrent du code Juste-à-temps (JIT) ou exécutent la mémoire à partir du segment ou de la pile de processus par défaut doivent accorder une attention particulière aux spécifications de la protection d'exécution. Le .NET Framework, par exemple, fonctionne avec le bit NX activé.

Les développeurs de pilotes sont encouragés à prévoir l'utilisation du mode PAE sur les plates-formes prenant en charge la protection d'exécution. Le comportement du mode PAE sur les systèmes Windows dotés d'un espace d'adressage physique de moins de 4 Go a été modifié pour réduire les incompatibilités de pilote.

Les applications qui tentent de violer la protection d'exécution déclenchent une exception avec le code d'état STATUS_ACCESS_VIOLATION (0xC0000005). Si une application nécessite de la mémoire exécutable, elle doit explicitement activer cet attribut sur la mémoire appropriée en spécifiant PAGE_EXECUTE, PAGE_EXECUTE_READ, PAGE_EXECUTE_READWRITE ou PAGE_EXECUTE_WRITECOPY dans l'argument de protection de la mémoire des fonctions d'allocation de mémoire virtuelle*.

Pour garantir la compatibilité avec NX, les applications qui nécessitent des zones de mémoire exécutables doivent utiliser les attributs PAGE_EXECUTE, PAGE_EXECUTE_READ, PAGE_EXECUTE_READWRITE ou PAGE_EXECUTE_WRITECOPY lors d'une allocation de mémoire. En outre, les applications ne peuvent pas s'exécuter à partir du segment de mémoire ou de la pile de processus par défaut. La plupart des applications qui exécutent des actions incompatibles avec la protection d'exécution devront être mises à jour pour être

entièrement compatibles.

Si une application alloue de la mémoire exécutable à partir d'un segment dédié, elle doit s'assurer que l'indicateur EXECUTE est activé sur ce segment de mémoire. Elle peut utiliser l'API VirtualAlloc() pour allouer la mémoire avec les paramètres de protection appropriés. Si une application n'alloue pas de la mémoire exécutable à partir d'un segment dédié, elle doit être modifiée pour le faire. L'application doit créer ce segment au moyen de l'API VirtualAlloc() et doit spécifier l'indicateur EXECUTE pour cette mémoire. Tout code généré doit être placé dans ce segment exécutable. Une fois le code exécutable généré, il est conseillé que l'application définisse des protections de mémoire pour interdire un accès WRITE à ce segment au moyen de l'API VirtualProtect(). Cela garantit une protection maximale pour les zones exécutables de l'espace d'adressage de processus.

Conclusion

Ce document préliminaire a décrit certaines des principales modifications que nous prévoyons d'apporter avec le Service Pack 2 de Windows XP pour améliorer la protection et la sécurité du système d'exploitation. La plupart de ces fonctions visent à atténuer la portée des attaques malveillantes contre les systèmes même lorsque les derniers correctifs n'ont pas encore été installés sur ces derniers. Certaines de ces modifications et améliorations peuvent avoir des implications pour les développeurs. Microsoft communique ces fonctionnalités à un stade précoce du processus afin que les développeurs apréhendent les implications de ces modifications et disposent du temps nécessaire pour apporter les changements éventuellement rendus nécessaires.

Microsoft reconnaît que les technologies de sécurité ne représentent qu'un aspect d'une stratégie de sécurité globale. Les technologies de sécurité décrites dans ce document s'inscrivent dans le cadre de l'initiative Trustworthy Computing visant à mieux immuniser les systèmes de nos clients.

Pour plus d'informations et pour obtenir d'éventuelles mises à jour de ce document, visitez le site Web MSDN Security Developer Center.

Informations complémentaires

Pour en savoir plus sur cette annonce, reportez-vous aux documents suivants :

- Communiqué de presse du 9 octobre 2003 : Microsoft Outlines New Initiatives in Ongoing Security Efforts To Help Customers
- Microsoft Outlines Ongoing Security Efforts to Help Customers

Ressources Microsoft relatives à la sécurité

- Abonnez-vous gratuitement aux bulletins de sécurité Microsoft pour obtenir les bulletins les plus récents (en langue anglaise).
- Internet Connection Firewall
- Microsoft Software Update Services

- Microsoft Systems Management Server
- Microsoft Baseline Security Analyzer
- Windows Server 2003 Reliability Enhancements
- Steps to help protect your PC

Ressources de sécurité TechNet

- TechNet Security
- Security Prescriptive Guidance from Microsoft
- Virus alerts
- Security antivirus information

Ressources de sécurité MSDN / développeur

- Security Developer Center
- Compiler Security Checks in Depth (/GS)
- Patterns & Practices for Developers
- Authentication in ASP.NET – .NET Security Guidance
- Improving Web Application Security – Threats and Countermeasures

Communauté Microsoft

Obtenez des informations relatives aux problèmes de sécurité proposées par des collègues et par les services Microsoft PSS (Product Support and Services).

- IT Pro Security Zone

Partenaires Microsoft

- Microsoft Security Partners
- Secure Network Connectivity Partners
- Streamline Security Management and Operations Partners
- Automate Information Access with Identity Management Partners

Ressources de support

- Support and Lifecycle Policy
- Pour une assistance et un support gratuits lors d'attaques par des virus ou des vers :
    - Aux États-Unis et au Canada, composez le 866-PC SAFETY (727-2338).
    - Dans d'autres pays/régions, contactez votre bureau Microsoft local

Les informations contenues dans ce document représentent l'opinion actuelle de Microsoft Corporation sur les points cités à la date de publication. Microsoft s'adapte aux conditions fluctuantes du marché et cette opinion ne doit pas être interprétée comme un engagement de la part de Microsoft ; de plus, Microsoft ne peut pas

garantir la véracité de toute information présentée après la date de publication.

Ce document est proposé à titre d'information seulement. MICROSOFT N'APPORTE AUCUNE GARANTIE EXPLICITE OU IMPLICITE QUANT AUX INFORMATIONS CONTENUES DANS CE DOCUMENT.

Haut de la page