

La gestion des correctifs de sécurité avec WinReporter et RemoteExec

Ce document décrit les fonctionnalités de WinReporter[®] et RemoteExec[®] permettant de maintenir les systèmes Windows[™] à jour en termes de correctifs de sécurité (Service Packs, hotfixes, etc.) afin de les protéger contre la plupart des attaques et virus.

L'application tardive des correctifs : la principale faille de sécurité de Windows

Le comblement rapide des vulnérabilités est un élément primordial pour assurer la sécurité d'un réseau informatique. Pour garantir la sécurité des systèmes, il n'est plus suffisant de contrôler de manière stricte les permissions des utilisateurs, d'activer les audits, et de stopper les services inutiles.

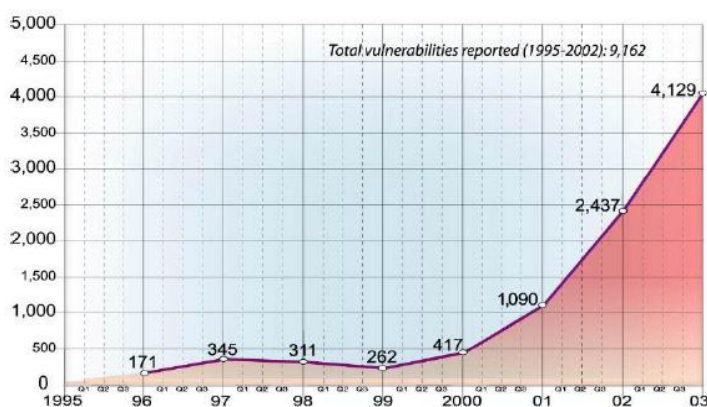
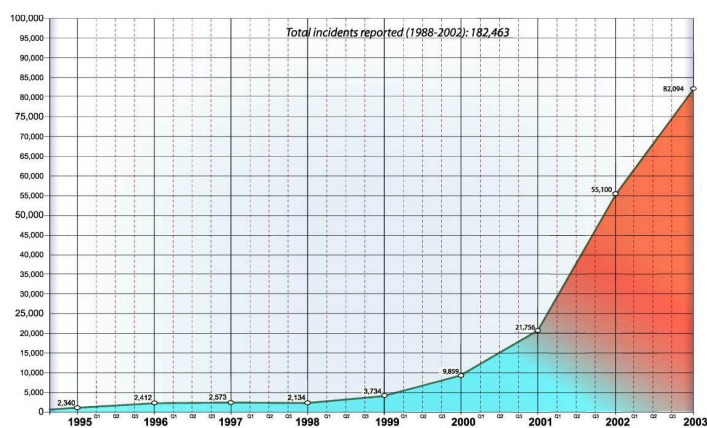
De nouvelles vulnérabilités sont divulguées chaque jour, fournissant autant d'occasions aux pirates de prendre en défaut la sécurité des réseaux.

Le SANS/FBI ⁽¹⁾ publie régulièrement la liste des 20 principales vulnérabilités réseau, et la majorité d'entre elles peuvent être facilement corrigées en appliquant simplement le correctif adéquat.

Par conséquent, la gestion des correctifs et des mises à jour doit devenir une activité quotidienne consistant à vérifier l'état des mises à jour des machines du réseau, et à déployer le plus rapidement possible les correctifs manquants. Cette gestion en continu est fondamentale pour garantir la protection du réseau.

L'expérience a trop souvent prouvé que les administrateurs appliquent tardivement les mises à jour, avec pour conséquence les effets dévastateurs des vers (Slammer, Blaster, Sobig, ...) exploitant ces vulnérabilités. Ces négligences coûtent des milliards de dollars aux entreprises chaque année.

Pour preuve, le centre de coordination du CERT ⁽²⁾ a publié une étude sur l'évolution des vulnérabilités et des incidents de sécurité depuis 1995 jusqu'à 2003 :



Deux observations: premièrement les deux courbes se superposent parfaitement, prouvant, si besoin en était, la corrélation entre ces deux paramètres, et deuxièmement, la progression de ces courbes est quasi exponentielle.

Cette situation est principalement due au fait que la gestion des mises à jour est une tâche pénible et longue. D'après une enquête d'Aberdeen Group ⁽³⁾, la gestion des mises à jour a coûté plus de 2 milliards de dollars en 2002, et ces chiffres vont continuer à augmenter.

(1) <http://www.sans.org/top20/> SANS/FBI: The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus

(2) <http://www.cert.org/>

(3) <http://www.aberdeengroup.com/2001/research/06030015.asp> Aberdeen Group, security perspective. Surfing the Security Patch Tidal Wave.

Gérer les mises à jour à l'aide de WinReporter® et RemoteExec®

Une gestion efficace des mises à jour (Service Packs, patches, hotfixes, ...) est donc un élément clé pour assurer la protection d'un réseau, puisque aucun ordinateur ne peut résister aux types d'attaques les plus récents si les mises à jour n'ont pas été dûment effectuées.

Cependant, l'application de certaines mises à jour peut créer de sérieux problèmes de compatibilité avec l'environnement informatique de production.

Par conséquent, il existe donc deux approches distinctes que les administrateurs peuvent adopter :

▶ *Le déploiement systématique des mises à jours*

Windows Update (WU) de Microsoft est un bon exemple d'outil utilisant cette approche, puisqu'il applique systématiquement toutes les nouvelles mises à jour, l'utilisateur n'ayant qu'à activer l'option des mises à jour automatiques sur sa machine.

Bien que cette alternative soit très pratique, l'administrateur n'a aucun moyen de contrôler quelles mises à jour sont appliquées sur les machines de son réseau, et doit donc avoir une confiance aveugle en Microsoft et en ses utilisateurs ...

▶ *L'approche adoptée par WinReporter® et RemoteExec®*

Cette approche consiste à tester les dernières mises à jour sur des ordinateurs de test, copies fidèles des serveurs et postes de travaux utilisés en production, avant de les déployer.

Cette approche est bien sûr plus laborieuse, mais c'est aussi la seule et unique façon d'éviter de sérieux déboires.

Le principal avantage de cette approche est de séparer les processus de vérification et de déploiement. WinReporter® propose des rapports détaillés fournissant une vision globale de la situation des mises à jour, et RemoteExec® permet un déploiement automatisé des mises à jours manquantes.

De plus, ces deux logiciels proposent des options qui font cruellement défaut à Windows Update :

WinReporter® :

- ▶ scanne les ordinateurs sélectionnés pour déterminer si une mise à jour donnée est appliquée ou non (Service Packs, patches, ou hotfixes)
- ▶ génère des rapports détaillés pour déterminer quelles sont les mises à jours manquantes
- ▶ génère des rapports permettant de s'assurer de la qualité de la sécurité du réseau concernant d'autres éléments (services, comptes, partages, permissions, ...)

RemoteExec® :

- ▶ déploie les mises à jour des versions de Windows même antérieures à Windows 2000
- ▶ déploie les mises à jour de logiciels tiers
- ▶ déploie les packages Windows Installer

WinReporter® & RemoteExec®: le duo gagnant

Scan des mises à jour avec WinReporter®

WinReporter® rapatrie, sans installation préalable d'agents sur les ordinateurs-cibles, toutes les informations indispensables à la compréhension du fonctionnement des réseaux (LAN et WAN) Windows et concernant :

- ▶ **Les matériels** : CPU, mémoire, BIOS, cartes vidéo, cartes réseaux (configuration TCP/IP), partitions, imprimantes, ...
- ▶ **Les logiciels** : applications installées, fichiers (avec versions et permissions), ...
- ▶ **Windows** : Service Packs, hotfixes, journaux d'événements, services, SAM (utilisateurs et groupes), partages, permissions sur les partages, ...
- ▶ **EventLogs** : analyse des journaux d'événements, démarrages et arrêts de postes de travail, accès fichiers, impressions, ...

et les stocke dans une base de données centrale de type ODBC (Access, SQL Server, Oracle, etc.).

Ces informations sont ensuite immédiatement exploitables :

- ▶ via 50 rapports pré-établis
- ▶ via l'utilisation de requêtes SQL personnalisées.

Pour détecter les ordinateurs vulnérables, WinReporter® propose la fonctionnalité suivante :

Rapports > Windows NT > Services Packs & hotfixes

A partir de ce panneau, les administrateurs peuvent détecter les ordinateurs non à jour. WinReporter® détecte les ordinateurs ayant (ou pas) la version de l'OS, le Service Pack, la version d'IE, le Service Pack IE, et enfin le hotfix choisis.

WinReporter® retourne la liste des ordinateurs correspondant aux critères pré-définis. Cette liste sera utilisée comme base pour déployer la mise à jour avec RemoteExec®.

Il y a deux façons de gérer l'analyse des mises à jour avec WinReporter® :

- ▶ Pour détecter les ordinateurs ayant un hotfix donné appliqué

Rapports > Général > Requête Générique, puis choisir la table hotfix.

WinReporter® retourne la liste des ordinateurs correspondant aux critères pré-définis.

- ▶ Pour obtenir un rapport complet sur l'état de mise à jour du réseau

Reports > Général > Global report

Au début de la partie correspondant aux ordinateurs on peut trouver le niveau du Service Pack appliqué, et, dans la sous partie hotfix, tous les hotfixes appliqués sont listés.

Si dans le cadre d'une bonne gestion des configurations, il est primordial de pouvoir déterminer l'état de la configuration d'un ordinateur à moment donné, ceci est aussi vrai pour l'état des mises à jour.

Dans l'éventualité d'un incident, il peut être important de savoir quel était l'état des mises à jour avant le problème afin de déterminer s'il existe une relation de cause à effet, ainsi que pour faciliter une rapide restauration du système.

Mise à jour distante avec RemoteExec®

RemoteExec® est un puissant outil d'administration à distance.

Ces fonctionnalités vont du redémarrage à distance jusqu'à l'exécution distante de programmes : les fonctionnalités de RemoteExec® dépassent donc largement le cadre du déploiement de mises à jour.

Bien que RemoteExec® laisse aux administrateurs la décision finale de déployer ou non les mises à jour, le processus de déploiement est rapide et pratique.

Premièrement il faut télécharger la mise à jour, puis l'appliquer sur la machine d'essai afin d'effectuer les tests nécessaires pour s'assurer que la mise à jour ne perturbe pas les systèmes existants.

Le déploiement sur les machines du réseau se fait ensuite en un seul clic.

Il est important de noter qu'il existe plusieurs types de mise à jour, voir *Microsoft Guide to Security Patch Management (page 27)*⁽⁴⁾. Par conséquent, chacune d'entre elles possède sa propre méthode de déploiement. RemoteExec® gère 5 types de mises à jour différentes:

- ▶ Service Packs et hotfixes pour systèmes d'exploitation
- ▶ Service Packs et hotfixes pour Internet Explorer
- ▶ Updates pour Microsoft Office, fichiers *.msp
- ▶ Les mises à jour Microsoft atypiques
- ▶ Les mises à jour de logiciels tiers

La valeur ajoutée de RemoteExec®

RemoteExec® se distingue des outils traditionnels de gestion des mises à jour dans la manière dont il assure les déploiements. Il déploie facilement les updates, hotfixes, et Services Packs de Microsoft, mais également les mises à jour de logiciels tiers.

Dans le cas où une intervention de l'utilisateur final est nécessaire, grâce à RemoteExec®, l'administrateur peut envoyer un popup, voire un message vocal (fichier *.wav par exemple) à tous ses utilisateurs pour les informer de la marche à suivre pour finaliser le déploiement. Ceci est un avantage différentiel important sur les logiciels qui ne gèrent que les mises à jour Microsoft.

Pour plus de sécurité, RemoteExec® fait la distinction entre mises à jour du système d'exploitation et mises à jour d'Internet Explorer.

Internet Explorer peut être vulnérable à de très nombreuses attaques, et une attention toute particulière doit donc être portée à sa mise à jour. Cette tâche est grandement facilitée par l'interface de RemoteExec® qui offre des champs différenciés pour le système d'exploitation et pour Internet Explorer.

Quelques avantages supplémentaires de RemoteExec® :

- ▶ RemoteExec® peut mettre à jour tous les systèmes Windows NT/2000/XP/2003 quels que soient leurs niveaux effectifs de Service Pack, et ne nécessite aucun logiciel tiers ou serveur dédié pour fonctionner.
- ▶ RemoteExec® consomme moins de bande passante Internet, puisqu'il distribue les mises à jour via le réseau. Les machines locales n'ont donc plus besoin d'accéder à Internet pour télécharger leurs mises à jour, d'où une économie de bande passante, et un meilleur contrôle des accès des machines vers l'extérieur du réseau.
- ▶ RemoteExec® permet de combler extrêmement rapidement les vulnérabilités exploitées par de nouveaux virus. Si un nouveau virus se dissémine rapidement sur Internet, et que la mise à jour correspondante n'est pas appliquée, l'administrateur n'aura qu'à sélectionner le correctif à appliquer pour déterminer les ordinateurs à mettre à jour, et avec un clic de plus le déploiement sera effectif.

N.B : Certains utilitaires comme par exemple Microsoft Baseline Security Analyzer (MBSA) ont une approche opposée, l'administrateur choisit d'abord la machine et obtient ensuite la liste des mises à jour de cette machine, ce qui n'est pas franchement pratique dans le cadre d'une mise à jour d'urgence.

(4) <http://microsoft.com/downloads/details.aspx?FamilyId=73AC38B7-5826-421D-99E8-CDCC608B8992&displaylang=en>
The Microsoft Guide to Security Patch Management

La valeur ajoutée de WinReporter®

WinReporter® facilite une gestion rigoureuse des mises à jour, en permettant aux administrateurs de connaître précisément et en temps réel la configuration de leur environnement : versions des logiciels installés, espace disque encore disponible, ou caractéristiques du matériel, ...

Ce type d'informations est particulièrement utile pour résoudre d'éventuels problèmes d'incompatibilité.

A contrario, et d'après Microsoft⁽⁵⁾ elle-même, les capacités de reporting de Windows Update (WU) ou de System Update Server (SUS) vont de « *pauvre* » à « *correcte* » ...

WinReporter® peut aussi faciliter le processus de récupération d'urgence : connaître la dernière configuration du système constitue une information précieuse pour rétablir rapidement un système opérationnel.

Le déploiement des mises à jour avec RemoteExec®

Voyons à présent comment appliquer avec RemoteExec® chacune des mises à jour évoquées ci-dessus.

Service Packs et hotfixes

Les procédures de déploiement des Service Pack et hotfixes pour le système d'exploitation et pour Internet Explorer sont pratiquement identiques :

- ▶ Clic droit sur *Action* et cocher *Hotfix/Mise à jour ou installation Service Pack*.
- ▶ Naviguer et sélectionner le fichier de mise de jour.
- ▶ La plupart des mises à jour renseignent automatiquement les champs de configuration d'action et filtre; cependant vous pouvez choisir votre propre configuration.
- ▶ Aller dans le volet *ordinateur*, et sélectionner les ordinateurs à mettre à jour.
- ▶ Lancer le déploiement.

Mise à jour d'une image administrative de Microsoft Office

La mise à jour de Microsoft Office est légèrement différente lorsque l'on utilise les images administratives.

- ▶ L'administrateur doit mettre à jour l'image administrative en lançant la commande *msiexec*.
- ▶ Ensuite RemoteExec® synchronise les ordinateurs du réseau pour compléter la mise à jour.

Microsoft⁽⁵⁾ donne un exemple bien documenté (voir *Administrative Update section*).

Mise à jour Microsoft atypique

Microsoft distribue parfois des mises à jour qui ne respectent pas la structure standard des hotfixes ou des Service Packs. Malgré cela, RemoteExec® peut les appliquer sans aucune difficulté.

Mise à jour de logiciels tiers

Le déploiement de mise à jour de logiciel tiers est légèrement différent.

- ▶ Clic droit *Type d'Action*, puis cocher *Exécution de fichiers*
- ▶ Naviguer et sélectionner le fichier de mise de jour.
- ▶ L'administrateur doit éventuellement l'éditeur du logiciel pour connaître les paramètres à introduire pour une exécution distante transparente.

(5) <http://support.microsoft.com/default.aspx?scid=kb:en-us:Q325671> The Microsoft XP Office updates deployment from server location (page 55)

Conclusion

De nouvelles failles de sécurité qui mettent en péril les réseaux d'entreprise sont découvertes chaque jour. Elles peuvent affecter aussi bien le système d'exploitation, qu'un logiciel intimement lié au système d'exploitation comme Internet Explorer, ou bien un logiciel tiers.

Malgré cela, les systèmes ne sont généralement pas mis à jour correctement, en particulier à cause de la charge de travail très conséquente que cela exige.

WinReporter® et RemoteExec® utilisés de concert facilitent considérablement cette mission cruciale de mise à jour, et de déploiement de correctifs : WinReporter® détecte rapidement les mises à jour manquantes, tandis que RemoteExec® les déploie facilement.

Enfin WinReporter® produit des rapports permettant de connaître la situation de la mise à jour du réseau à un moment déterminé.