Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 07 décembre 2000
N° CERTA-2000-AVI-085

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités des bases de registres de Windows NT et 2000

Gestion du document

Référence	CERTA-2000-AVI-085
Titre	Vulnérabilités des bases de registres de Windows NT et 2000
Date de la première version	07 décembre 2000
Date de la dernière version	–
Source(s)	Bulletins de sécurité Microsoft
Pièce(s) jointe(s)	Aucune

TAB. 1 – *gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Compromission de machine ;
- augmentation des privilèges ;
- prise de contrôle à distance ;
- exécution de code arbitraire.

2 Systèmes affectés

Windows NT 4.0 et Windows 2000.

3 Résumé

Des permissions par défaut inadéquates de certaines clés de la base de registres de Windows NT et 2000, permettent à un utilisateur malicieux de prendre le contrôle de services tels que la gestion de SNMP (*Simple Network Management Protocol* = gestion et observation des fonctionnalités réseau d'une machine), RAS (*Remote Access Server* = Service d'accès au réseau à distance) et la gestion des modules de MTS (*Microsoft Transaction Server* = service de gestion des transaction).

4 Description

Des vulnérabilités de la base de registres de Windows NT 4.0 permettaient à un utilisateur mal intentionné, ayant accès localement à la machine, d'obtenir les clés de chiffrement des autres utilisateurs ayant eu accès précédemment à cette machine et d'exécuter du code arbitraire avec les privilèges de l'utilisateur `Système`. Ces vulnérabilités liées à des permissions insuffisantes de plusieurs clés de la base des registre, avaient été traitées par Microsoft dans les bulletins MS99-025, MS00-008 et MS00-024.

- La clé `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug` (HKLM=HKEY_LOCAL_MACHINE) qui est utilisée par l'administrateur pour spécifier un débogueur distant qui sert à faire établir un diagnostic par la machine distante en cas d'arrêt brutal et inopiné de la machine locale. Des permissions laxistes sur cette clé permettent à n'importe quel utilisateur mal intentionné de faire lancer un autre programme de son choix à la place du débogueur. Il lui suffit de provoquer un arrêt inopiné sur la machine à compromettre pour exécuter son code avec les privilèges système.
- La clé `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders` fournit des informations sur l'emplacement de multiples répertoires partagés par tous les utilisateurs sur une machine.
  Parmi les clés filles de celle-ci, l'une d'entre elles spécifie un répertoire de démarrage commun (common startup folder). Cette clé possède des permissions trop simples, permettant à un utilisateur mal intentionné de changer le répertoire destination, de façon à ce que du code malicieux soit exécuté lors de l'ouverture de la session suivante.
- Les clés `HKLM\SOFTWARE\Microsoft\DataFactory` et `HKLM\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch` déterminent les paramètres de sécurité pour les services de base de données. Leurs valeurs pouvant être changées par n'importe quel utilisateur ayant ouvert une session localement, les mesures de sécurité peuvent être désactivées.
- La clé `HKLM\SOFTWARE\Microsoft\Cryptography\Offload` est une clé utilisée par une fonction du module *CryptoAPI* appelé lors de hachages ou de chiffrements de données par les services de chiffrements.

D'autres vulnérabilités de la base de registres de Windows NT 4.0 et Windows 2000 permettent à un utilisateur mal intentionné d'exécuter du code avec des privilèges de `Système` ou de prendre le contrôle du système.

- La clé `HKLM\SYSTEM\CurrentControlSet\Services\SNMP\Parameters` de la base de registres de Windows NT 4.0 et Windows 2000 est visible et modifiable par toute personne ayant accès à la machine. Cette clé permet à un utilisateur mal intentionné d'obtenir des informations sur la communauté SNMP (cf. RFC 1157) à laquelle appartient sa machine, et d'ajouter des communautés SNMP auxquelles il appartient et ayant des privilèges d'administration. Pour windows NT, cette vulnérabilité est exploitable à distance, alors qu'elle ne l'est pas (par défaut) sous windows 2000.
- La clé `HKLM\SOFTWARE\Microsoft\RAS` de la base de registres de Windows NT 4.0 permet aux administrateurs d'utiliser un produit tiers comme extension du service d'accès à distance. RAS et ses extensions fonctionnent avec les privilèges du groupe `Système`. Cette clé est visible et modifiable par un utilisateur sans privilèges sous Windows NT 4.0 uniquement, ce qui permet à un utilisateur mal intentionné d'ajouter un produit de sa conception comme extension de RAS.
  Son programme, considéré alors comme une extension de RAS, s'exécutera avec les privilèges de `Système`.
  `Nota` : Pour que ce programme puisse être associé à RAS, il faut que l'utilisateur malicieux installe une bibliothèque partagée (DLL) dont les points d'entrées correspondent à ceux d'un outil d'administration de RAS légitime.
- La clé `HKLM\SOFTWARE\Microsoft\Transaction Server\Packages` de la base de registres de Windows NT 4.0, et les autres clés de son arborescence, permettent de créer et de gérer des modules de transaction de MTS. Les modules sont des ensembles de logiciels intervenant ensemble, en fonction de certains évènements, dans le déroulement d'une transaction. (début, fin, succès, échec...).
  Un utilisateur mal intentionné ayant un accès local à la machine peut, en modifiant ces clés, remplacer un module de transaction par un de sa confection, détournant ainsi les transactions de ce serveur à son avantage.

SNMP, RAS et MTS ne sont pas installés par défaut sous Windows NT ou Windows 2000.

5 Recommandation

Un serveur, ne doit autoriser à ouvrir une session locale à aucun autre utilisateur que celui qui l'administre.

6 Solution

Appliquer le correctif Microsoft :

- Pour Windows 2000 (Seule la vulnérabilité de SNMP est concernée) :
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24500
- Pour Windows NT, le correctif couvre toutes les vulnérabilités énumérées ci-dessus :
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24501

Ou bien exécuter à la main les changements de permissions dans la base de registres à l'aide de l'outils `regedt32.exe` :

Le tableau récapitulatif suivant (cf. table 2) résume les permissions qui doivent êtres appliquées à chaque clé de la base de registres.

Branche	Clé	Permissions
`HKLM\SOFTWARE`	`Microsoft\Windows NT\CurrentVersion\ AeDebug`	**Utilisateurs authentifiés** : lecture seule ; **Administrateurs** : Contrôle total ; **Système** : Contrôle total ; **Créateur Propriétaire** : Contrôle total.
`HKLM\SOFTWARE`	`Microsoft\Windows\CurrentVersion \Explorer\User Shell Folders`	**Utilisateurs authentifiés** : lecture seule ; **Administrateurs** : Contrôle total ; **Système** : Contrôle total ; **Créateur Propriétaire** : Contrôle total.
`HKLM\SOFTWARE`	`Microsoft\DataFactory`	**Utilisateurs authentifiés** : lecture seule ; **Administrateurs** : Contrôle total ; **Système** : Contrôle total ; **Créateur Propriétaire** : Contrôle total.
`HKLM\SYSTEM`	`CurrentControlSet\Services\W3SVC\ Parameters\ADCLaunch`	**Utilisateurs authentifiés** : lecture seule ; **Administrateurs** : Contrôle total ; **Système** : Contrôle total ; **Créateur Propriétaire** : Contrôle total.
		.../...

.../... Branche	Clé	Permissions
HKLM\SYSTEM	CurrentControlSet\Control\ SecurePipeServers\winreg	**Administrateurs** : sauvegarde complète ; **Operateurs de serveur** : lecture seule.
HKLM\SOFTWARE	Microsoft\Cryptography\Offload	**Utilisateurs authentifiés** : lecture seule ; **Administrateurs** : Contrôle total ; **Système** : Contrôle total ; **Créateur Propriétaire** : Contrôle total.
HKLM\SOFTWARE	Microsoft\Transaction Server\Packages	**Administrateurs** : Contrôle total ; **Système** : Contrôle total ; **Créateur Propriétaire** : Contrôle total.
HKLM\SOFTWARE	Microsoft\RAS	**Administrateurs** : Contrôle total ; **Système** : Contrôle total ; **Créateur Propriétaire** : Contrôle total.
HKLM\SYSTEM	CurrentControlSet\Services\SNMP\ Parameters\ValidCommunities	**Administrateurs** : Contrôle total ; **Système** : Contrôle total ; **Créateur Propriétaire** : Contrôle total.
HKLM\SYSTEM	CurrentControlSet\Services\SNMP\ Parameters\PermittedManagers	**Administrateurs** : Contrôle total ; **Système** : Contrôle total ; **Créateur Propriétaire** : Contrôle total.

TAB. 2 – *Permissions des clés de la base de registres*

Nota : Les permissions de la clé HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg, qui est utilisée dans l'accès à distance de la base de registres, sont aussi à modifier.

Ce tableau peut aussi permettre de vérifier que le correctif Microsoft à bien effectué ces changements.

7 Documentation

- Bulletin de Sécurité Microsoft MS00-095 et sa FAQ :
  http://www.microsoft.com/technet/security/bulletin/ms00-095.asp
  http://www.microsoft.com/technet/security/bulletin/fq00-095.asp
- Bulletin de Sécurité Microsoft MS00-096 et sa FAQ :
  http://www.microsoft.com/technet/security/bulletin/ms00-096.asp
  http://www.microsoft.com/technet/security/bulletin/fq00-096.asp

- Bulletin de Sécurité Microsoft MS00-008 et sa FAQ :
  http://www.microsoft.com/technet/security/bulletin/ms00-008.asp
  http://www.microsoft.com/technet/security/bulletin/fq00-008.asp
- Bulletin de Sécurité Microsoft MS00-024 et sa FAQ :
  http://www.microsoft.com/technet/security/bulletin/ms00-024.asp
  http://www.microsoft.com/technet/security/bulletin/fq00-024.asp
- Bulletin de Sécurité Microsoft MS99-025 (1999) et sa FAQ :
  http://www.microsoft.com/technet/security/bulletin/ms99-025.asp
  http://www.microsoft.com/technet/security/bulletin/fq99-025.asp
- l'article de Microsoft concernant les restrictions sur l'accès à distance à une base de registres :
  http://support.microsoft.com/support/kb/articles/Q153/1/83.asp

Gestion détaillée du document

07 décembre 2000 version initiale.