Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 mars 2002
N° CERTA-2002-AVI-033-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du service `SNMP` sous Microsoft Windows

Conditions d'utilisation de ce document : `http://www.certa.ssi.gouv.fr/certa/apropos.html`
Dernière version de ce document : `http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-033`

Gestion du document

Référence	CERTA-2002-AVI-033-001
Titre	Vulnérabilité du service `SNMP` sous Microsoft Windows
Date de la première version	13 février 2002
Date de la dernière version	15 mars 2002
Source(s)	Bulletin de sécurité Microsoft MS02-006 Bulletin d'alerte du CERTA-2002-ALE-004
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

Exécution de code arbitraire à distance.

2 Systèmes affectés

Microsoft Windows 9x, ME, XP, NT et 2000.

3 Résumé

Un utilisateur mal intentionné peut utiliser une vulnérabilité de l'agent SNMP sous Microsoft Windows pour exécuter du code arbitraire à distance avec les privilèges de l'administrateur du système.

Le bulletin de sécurité de Microsoft à été mis à jour suite à l'ajout de correctifs et à une erreur dans l'implémentation de plusieurs correctifs.

4 Description

Les tests effectués par l'université finlandaise d'Oulu ont mis en évidence la présence de vulnérabilités dans les routines de décodage et de traitement des messages SNMP dans de nombreuses implémentations (se référer au bulletin d'alerte CERTA-2002-ALE-004 du CERTA).

Une vulnérabilité de l'agent SNMP, permet à un utilisateur mal intentionné d'exécuter du code arbitraire avec les privilèges de l'administrateur du système. Cette vulnérabilité, de type débordement de mémoire, est exploitable à distance.

Des correctifs pour les systèmes Microsoft qui n'étaient pas encore disponibles lors de la première version de cet avis ont été ajoutés le 5 mars 2002 pour Windows NT 4.0 server et le 11 mars pour Windows NT 4.0 Terminal Server Edition.

Pour des raisons de disponibilité et de moindres effets de bords des correctifs, il est souvent plus judicieux d'installer les systèmes des serveurs dans leur langue de développement (ici l'anglais). Cependant suite à la détection d'erreurs dans les correctifs pour les versions anglaise et allemande de Windows NT 4.0 Terminal Server Edition, Microsoft a modifié ces dernières.

Les administrateurs de systèmes Microsoft Windows Terminal Server Edition installés en langue anglaise sont donc invités à aller télécharger la nouvelle version du correctif.

5 Contournement provisoire

- S'il n'est pas utilisé, ou en attendant d'obtenir le correctif, désactiver `SNMP`.
  Pour vérifier si le service `SNMP` est installé et démarré et l'arrêter s'il existe, procéder de la façon suivante :
  - Pour Windows 9x :
    1. Dans le `panneau contrôle` ouvrir les paramètres du `réseau`.
    2. Cliquer sur l'onglet `configuration` et sélectionner `Agent SNMP` dans la liste des composants installés.
    3. cliquer sur le bouton `supprimer`.
  - Pour Windows NT 4.0 (Terminal server compris) :
    1. Dans le `panneau contrôle` ouvrir les paramètres du `services`.
    2. Sélectionner le service `SNMP`, cliquer sur le bouton `arrêter`.
    3. Dans la liste des modes de démarrage (en dessous), cliquer sur le bouton `Désactivé`.
    4. Puis cliquer sur `OK` pour fermer cette fenêtre.
  - Sous Windows 2000 and XP :
    1. Ouvrir la `Gestion de l'ordinateur` dans les `Outils d'administration` ;
    2. Choisir `Services et Applications`, puis `Services` ;
    3. Sélectionner le service `SNMP`, cliquer sur le bouton `arrêter`.
    4. Dans la liste des modes de démarrage, sélectionner `Désactivé`.
    5. Puis cliquer sur `OK` pour fermer, puis fermer la fenêtre d'administration.
- filtrer le port 161/UDP utilisé par l'agent `SNMP` au niveau du garde-barrière afin d'empêcher l'exploitation de ces vulnérabilités depuis l'Internet.

6 Solution

Se référer au bulletin de Microsoft MS02-006 pour le disponibilité des correctifs.

7 Documentation

- Le bulletin de sécurité Microsoft MS02-006 :
  http://www.microsoft.com/technet/security/bulletin/MS02-006.asp
- L'alerte du CERTA : CERTA-2002-ALE-004.

Gestion détaillée du document

13 février 2002 version initiale.

25 février 2002 première révision : erreur dans la numérotation (tableau *Gestion du Document* et balise *reference*).

15 mars 2002 seconde révision : ajout de correctifs Microsoft et erreur dans le correctif en version anglaise et allemande concernant Windows NT Server Terminal Edition