Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 mai 2001
N° CERTA-2001-ALE-007

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Propagation d'un ver affectant sadmind et IIS

Gestion du document

Référence	CERTA-2001-ALE-007
Titre	Propagation d'un ver affectant sadmind et IIS
Date de la première version	09 mai 2001
Date de la dernière version	–
Source(s)	CERT-CC
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 des machines Solaris avec sadmind et Windows avec IIS.

2 Systèmes affectés

- Tous les systèmes avec les versions 4.0 et 5.0 non mises à jour de Internet Information Server (IIS) ;
- Tous les systèmes Solaris de 2.3 à 7 non mis à jour.

3 Résumé

Un nouveau ver se propage en exploitant des vulnérabilités assez anciennes de Sun Solaris et de IIS. Celui-ci permet l'obtention de privilèges administrateur à distance.

4 Description

Ce nouveau ver exploite deux failles assez connues pour se propager.
Il se propage sur les systèmes Solaris par la vulnérabilité de sadmind connue depuis décembre 1999.

Après avoir piraté le système Solaris, le ver ajoute la ligne « + + » dans le fichier .rhosts qui se trouve dans le répertoire de l'utilisateur root.

Il installe ensuite des outils pour exploiter la vulnérabilité d'IIS connue depuis octobre 2000 (sous le nom "Web Server Folder Traversal").

Il modifie ensuite le fichier index.html du système sur lequel il se trouve après avoir piraté 2000 serveurs IIS.

Un système Solaris compromis par ce ver contient normalement :

- Une fenetre de commande avec les privilèges administrateur en écoute sur le port 600/tcp ;
- le répertoire /dev/cub qui contient des logs de machines piratées ;
- le répertoire /dev/cuc qui contient les outils d'attaque.

5 Contournement provisoire

Veiller à bloquer le trafic à destination du port 111/tcp (sunrpc - portmapper, nécessaire à l'exploitation de la faille sadmind).

6 Solution

Appliquer les patches correctifs qui se trouvent sur les liens :

- Pour IIS 4.0 :
  http://www.microsoft.com/ntserver/nts/downloads/critical/q269862/default.asp
- Pour IIS 5.0 :
  http://www.microsoft.com/windows2000/downloads/critical/q269862/default.asp
- Pour sadmind :
  http://www.sunsolve.com/pub-cgi/retrieve.pl?doctype=coll&doc=secbull/191&type=0&nav=sec.sba
- Si la machine est compromise, prendre contact avec le CERTA.

7 Documentation

Bulletin du CERT-CC :
http://www.cert.org/advisories/CA-2001-11.html

Gestion détaillée du document

09 mai 2001 version initiale.