Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 août 2000
N° CERTA-2000-AVI-029

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Faille dans le démon telnetd sous IRIX de SGI

Gestion du document

Référence	CERTA-2000-AVI-029
Titre	Faille dans le démon telnetd sous IRIX de SGI
Date de la première version	17 août 2000
Date de la dernière version	–
Source(s) –	Avis de sécurité SGI 20000801-01-A du 1/08/2000 Avis CERT-IST/AV-2000.186 du 16/08/2000
Pièce(s) jointe(s)	Aucune

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

1 Risque

- Exécution de code arbitraire permettant à un utilisateur distant l'accès avec les privilèges *root*.
- Déni de service

2 Systèmes affectés

- Système d'exploitation IRIX versions 6.2 à 6.5.8 de Silicon Graphics (SGI).
- Versions 5.2 à 6.0.1 d'IRIX ayant reçue le patch 1020, version 6.1 d'IRIX ayant reçue le patch 1010.

3 Résumé

Le démon *telnetd* ne vérifie pas correctement certaines variables d'environnement transmises par le client. Un utilisateur mal intentionné peut fabriquer une requête provoquant un débordement de pile et exécuter du code arbitraire sur la machine avec les privilèges de *root*.

Une exploitation de cette vulnérabilité a été publiée sur Internet.

4 Description

Cette vulnérabilité a été introduite par les correctifs publiés (patchs 1010 et 1020) suite à l'avis du CERT/CC CA-95.14 qui concernait déjà des problèmes de variables d'environnement telnet. Cette correction a été reconduite dans les nouvelles versions du système d'exploitation.

Les versions 5.2 à 6.1 non patchées ne sont donc pas vulnérables à ce problème, mais le sont cependant à ceux de l'avis du CERT/CC.

5 Contournement provisoire

Il s'agit de désactiver le service *telnet* sur la machine.
Mode opératoire :

- se connecter en tant qu'administrateur *root*,
- éditer le fichier de configuration d'*inetd* "*/etc/inetd.conf*" : commenter la ligne *telnet stream tcp nowait root /usr/etc/telnetd telnetd*
- forcer *inetd* à relire son fichier de configuration : */etc/killall -HUP inetd*,
- détruire les connections telnet en cours : */etc/killall telnetd*.

6 Documentation

- Bulletin de sécurité SGI 20000801-01-A
  ftp://sgigate.sgi.com/security/20000801-01-A
- Copie du message BugTraq
  http://msgs.securepoint.com/cgi-bin/get/bugtraq0008/152.html

Gestion détaillée du document

17 août 2000 version initiale.