Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 juin 2001
N° CERTA-2001-AVI-062

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Xinetd

Gestion du document

Référence	CERTA-2001-AVI-062
Titre	Vulnérabilité de Xinetd
Date de la première version	11 juin 2001
Date de la dernière version	–
Source(s)	Avis de sécurité RHSA-2001:075-05
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

- Déni de service,
- Obtention du privilège root à distance,
- Compromission de données.

2 Systèmes affectés

Toutes les versions de xinetd antérieures à 2.1.8.9pre15.
Distributions RedHat 7.0 et RedHat 7.1.

3 Résumé

Un débordement de mémoire dans le serveur xinetd permet à un utilisateur mal intentionné de provoquer un déni de service (arrêt brutal du processus) voire d'exécuter du code à distance.

En outre, dans le paquetage d'installation de la distribution RedHat (Redhat 7.0 et RedHat 7.1), un mauvais positionnement des droits d'accès par défaut peut entraîner, dans certains cas, la possibilité de lire ou de modifier des fichiers générés par les services démarrés au moyen de xinetd.

4 Description

Le service xinetd (eXtended InterNET services Daemon) est le successeur du service inetd.
Ce service contôle le démarrage d'autres services (ftpd, telnetd ...).

4.1 Débordement mémoire dans xinetd.

Xinetd permet d'enregistrer, après l'interrogation du service identd de la machine distante, l'identité de l'utilisateur accédant aux différents services.

Un utilisateur mal intentionné peut utiliser sur sa machine un service identd forgeant une réponse qui provoquera un débordement mémoire sur le service xinetd distant .

Si aucune exploitation de cette vulnérabilité n'a été publiée en vue de l'obtention du privilège root à distance, l'occurence d'un débordement mémoire peut toutefois entraîner l'arrêt intempestif du service xinetd, empêchant de ce fait le démarrage des services gérés par ce dernier.

4.2 Mauvais positionnement des droits d'accès par défaut.

Dans les distributions Redhat 7.0 et 7.1, xinetd utilise le masque par défaut `umask 0`.

Les services démarrés par xinetd et qui ne positionnent pas eux-même les droits d'accès aux fichiers créés, vont créer des fichiers avec les droits de lecture et d'écriture pour tout le monde.

5 Solution

Télécharger le correctif disponible sur le site de RedHat :

– ftp://updates.redhat.com/7.0/en/os/SRPMS/xinetd-2.1.8.9pre15-2.src.rpm

– ftp://updates.redhat.com/7.1/en/os/SRPMS/xinetd-2.1.8.9pre15-2.src.rpm

Ce paquetage contient la nouvelle version d'xinetd (version Xinetd 2.1.8.9pre15) et corrige aussi le problème lié au positionnement des droits d'accès par défaut.

6 Documentation

Avis de sécurité RHSA-2001:075-05

Gestion détaillée du document

11 juin 2001 version initiale.