Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 mai 2001
N° CERTA-2001-AVI-051

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Vixie Cron

Gestion du document

Référence	CERTA-2001-AVI-051
Titre	Vulnérabilité de Vixie Cron
Date de la première version	14 mai 2001
Date de la dernière version	–
Source(s)	Avis Debian DSA-054-1 cron
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

Obtention du privilège root en local. Des programmes exploitant cette vulnérabilité ont été publiés.

2 Systèmes affectés

- Linux Debian 2.2
- Linux Mandrake 7.1, 7.2, 8.0, Corporate Server 1.0.1

3 Résumé

Une correction apportée à une précédente vulnérabilité de Vixie Cron, introduit une nouvelle vulnérabilité permettant à une personne mal intentionnée d'obtenir les privilèges root en local.

4 Description

Cron est un outil permettant à un utilisateur de planifier l'exécution de tâches périodiquement ou à des heures précises.

La version de cron publiée pour apporter une correction à une précédente vulnérabilité décrite dans l'avis `CERTA-2000-AVI-076` paru en novembre 2000, introduit une nouvelle vulnérabilité.

Si une erreur est rencontré dans l'analyse du fichier crontab après sa modification, crontab ne réduit pas immédiatement ses privilèges d'exécution (crontab est installé avec le bit setuid root). Ainsi, il est possible pour un utilisateur mal intentionné de lancer l'édition sous crontab (`crontab -e`) avec un éditeur qui va générer une erreur d'analyse puis exécuter des commandes arbitraires avec les privilèges de root.

5 Contournement provisoire

Restreindre l'accès à l'utilitaire cron aux utilisateurs de confiance via les fichiers `/etc/cron.allow` et `/etc/cron.deny` (se référer à l'aide en ligne: `man crontab`).

6 Solution

Des correctifs sont disponibles sur les sites des différents éditeurs:

- http://www.debian.org/security/2001/dsa-054
- http://www.linux-mandrake.com/en/security/2001/MDKSA-2001-050

7 Documentation

Avis de Sécurité Debian:
http://www.debian.org/security/2001/dsa-054

Gestion détaillée du document

14 mai 2001 version initiale.