

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Vixie Cron

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-2000-AVI-076>

Gestion du document

Référence	CERTA-2000-AVI-076
Titre	Vulnérabilité de Vixie Cron
Date de la première version	23 novembre 2000
Date de la dernière version	–
Source(s)	Debian
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

Accès *root* en local. Une exploitation de la vulnérabilité a été publiée.

2 Systèmes affectés

Linux Debian.

Probablement d'autres distributions sont touchées, renseignez vous auprès du distributeur.

3 Résumé

Une vulnérabilité est présente dans Vixie Cron sous debian. D'autres distributions de Linux peuvent être touchées. Elle permet d'obtenir des privilèges *root* en local.

4 Description

Cron est un outil permettant de planifier l'exécution de tâches à heures précises ou périodiquement. Une vulnérabilité dans la gestion des fichiers temporaires par `crontab` lors de la programmation des tâches (`crontab -e` permet à un utilisateur local mal intentionné de faire exécuter par `crond` le code qu'il désire avec les permissions du propriétaire de la tâche programmée. Si le propriétaire de la tâche qui est exécutée est `root`, le code sera exécuté avec les privilèges de ce dernier. Des exploitations de cette vulnérabilités permettent entre autre d'obtenir un *shell root*.

5 Contournement provisoire

Affiner les permissions d'accès du répertoire `crontabs` :

```
chmod go-rx /var/spool/cron/crontabs
```

en tant que *root*.

6 Solution

Appliquer le correctif proposé sur le site Debian :
<http://secutity.debian.org/dists/potato/updates/main>
Le correctif à télécharger s'appelle `cron_3.0p11-57.1_[arch].deb` où `[arch]` peut être : `i386` (pour architecture intel), `arm`, `alpha`, `powerpc`, `mk68k` ou `sparc`.

7 Documentation

Avis de sécurité de Debian :
<http://www.debian.org/security/2000/20001118a>

Gestion détaillée du document

23 novembre 2000 version initiale.