

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans « Workshop » cvconnect sous IRIX

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-012>

Gestion du document

Référence	CERTA-2000-AVI-012
Titre	Vulnérabilité dans « Workshop » cvconnect sous IRIX
Date de la première version	29 juin 2000
Date de la dernière version	–
Source(s)	Avis K-056 du CIAC
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

Ecrasements de fichiers.

De façon générale, un écrasement de fichier peut avoir pour conséquences : une destruction de la configuration de la machine, un accès root à la machine, etc.

2 Systèmes affectés

IRIX 5.3 et 6.1 à 6.5 munis des outils « Workshop Debugger and Performance » versions 2.6 et inférieures.

3 Résumé

Workshop est une suite logicielle d'outils aidant les développeurs à mettre au point les programmes. Le programme « cvconnect » est appelé par ce logiciel.

Une vulnérabilité dans « cvconnect » a été découverte, autorisant n'importe quel utilisateur à l'exécuter.

4 Description

Dans son utilisation normale, « cvconnect » n'est pas utilisé manuellement par l'utilisateur, mais appelé par le fonctionnement de la suite logicielle « WorkShop » .

Or, il a été découvert qu'il est possible à n'importe quel utilisateur possédant un compte local d'exécuter la commande manuellement, en local ou à distance. Cette commande permet à un utilisateur mal intentionné d'écraser n'importe quel fichier du système.

5 Contournement provisoire

Après avoir vérifié la version de « WorkShop », il faut, en ayant accès en root à la machine, supprimer les permissions nuisibles à « cvconnect » .

Pour vérifier la version, utiliser la commande 'version' :

```
# version -b WorkShop
```

Pour changer les permissions de « cvconnect », utiliser la commande 'chmod' :

```
# /bin/chmod 500 /usr/lib/WorkShop/cvconnect
```

Vérifier les nouvelles permissions :

```
# ls -l /usr/lib/WorkShop/cvconnect
```

```
-r-x----- 1 root sys 428664 Sep 11 1997 cvconnect
```

6 Solution

Il existe une version 2.7 de « WorkShop » qui corrige le problème. Il faut donc mettre à jour la version de « WorkShop ».

Nota : Cette mise à jour n'est possible que sur les versions 6.2 à 6.5 d'IRIX. Pour les versions 5.3 et 6.1, il faut : soit mettre à jour le système, soit faire la manipulation décrite dans le paragraphe 5.

7 Documentation

Avis du CIAC :

<http://www.ciac.org/ciac.bulletins/k-056.shtml>

Gestion détaillée du document

29 juin 2000 version initiale.