Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 novembre 2000
N° CERTA-2000-AVI-075

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du logiciel InPerson sous IRIX

Gestion du document

Référence	CERTA-2000-AVI-075
Titre	Vulnérabilité du logiciel InPerson sous IRIX
Date de la première version	22 novembre 2000
Date de la dernière version	–
Source(s)	BugTraq FAQ de SGI IRIX
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.

2 Systèmes affectés

Tous les systèmes IRIX ayant l'outil InPerson installé.

3 Résumé

Un utilisateur mal intentionné peut, en utilisant une vulnérabilité de InPerson, obtenir les privilèges root. L'exploitation de cette vulnérabilité a largement été diffusée sur internet.

4 Description

InPerson est un logiciel de visioconférence proposé par défaut lors de l'installation du système IRIX sur une station ou un serveur Silicon Graphix.

Un mauvais paramétrage par défaut des permissions de la commande `inpview` permet à un utilisateur mal intentionné d'exécuter un *shell* avec les privilèges de root et, par conséquent, de prendre possession de la machine.

5 Solution

On peut savoir si InPerson (toutes les versions de InPerson sont vulnérables) est installé en demandant au système sa version de la façon suivante :

En tant que `root`, taper la commande suivante :

```
versions -b InPerson
```

Le numéro de la version apparaît à la fin de la description affichée.

Si le logiciel InPerson est installé, et si vous ne l'utilisez pas, il faut le supprimer à l'aide de la commande suivante :

```
versions remove InPerson
```

Si vous utilisez InPerson sur cette station, il faut supprimer le bit `SUID` de la commande `inpview` en exécutant la commande suivante :

```
chmod u-s /usr/lib/InPerson/inpview
```

Vous pouvez en plus restreindre l'accès au logiciel à un seul groupe d'utilisateurs qui a accès localement à la station pour utiliser le logiciel, et que vous aurez créé sur la machine, grâce à la commande `chgroup`.

6 Documentation

Aucune documentation n'est disponible actuellement.

Gestion détaillée du document

22 novembre 2000 version initiale.