



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 mai 2004
N° CERTA-2004-AVI-175

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la bibliothèque libcpr 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-2004-AVI-175>

Gestion du document

Référence	CERTA-2004-AVI-175
Titre	Vulnérabilité dans la bibliothèque libcpr sous Irix
Date de la première version	27 mai 2004
Date de la dernière version	-
Source(s)	Avis de sécurité SGI
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

Elévation de privilèges.

2 Systèmes affectés

SGI Irix versions antérieures à la version 6.5.25.

3 Résumé

Une vulnérabilité présente dans la bibliothèque libcpr permet à un utilisateur local mal intentionné d'obtenir les privilèges du super-utilisateur root.

4 Description

`/usr/sbin/cpr` est une commande livrée avec le paquetage `coe.sw.cpr` (IRIX Checkpoint and Restart) installé par défaut sur les systèmes IRIX 6.5.x.

Une vulnérabilité sur la bibliothèque libcpr permet à un utilisateur non privilégié de redémarrer un processus. Cette vulnérabilité permet à un utilisateur mal intentionné d'obtenir les privilèges du super-utilisateur root.

5 Solution

Appliquer les correctifs ou mettre à jour votre système avec la version d'Irix 6.5.25 (cf. section documentation).

6 Documentation

- Avis de sécurité SGI :
<ftp://patches.sgi.com/support/free/security/advisories/20040507-01-P.asc>
- Référence CVE CAN-2004-0134 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0134>

Gestion détaillée du document

27 mai 2004 version initiale.