



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 février 2003
N° CERTA-2003-AVI-033

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Débordement de pile sur la commande ps

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-2003-AVI-033>

Gestion du document

Référence	CERTA-2003-AVI-033
Titre	Débordement de pile sur la commande ps
Date de la première version	28 février 2003
Date de la dernière version	–
Source(s)	Avis de sécurité CSSA-2003-SCO.1.1 de SCO Security
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

- Exécution de code arbitraire en local ;
- élévation de privilèges.

2 Systèmes affectés

- UnixWare 7.1.1 ;
- Open Unix 8.0.0 ;
- UnixWare 7.1.3 ;
- Irix 6.5.5 et versions antérieures.

3 Résumé

Un débordement de pile présent sur la commande `ps` permet à un utilisateur local d'exécuter un code arbitraire avec les privilèges du système.

4 Description

Une vulnérabilité de type débordement de pile à été découverte sur la commande `ps`. Elle permet à un utilisateur mal intentionné d'exécuter du code arbitraire avec les privilèges du système. Cette vulnérabilité n'est exploitable qu'en local.

5 Solution

Appliquer le correctif correspondant à votre système (cf section documentation).

6 Documentation

- Avis de sécurité CSSA-2003-SCO.1.1 de SCO Security
<ftp://ftp.sco.com/pub/updates/OpenUNIX/CSSA-2003-SCO.1.1/CSSA-2003-SCO.1.1.txt>
- Correctif pour Irix 6.5.x
<http://support.sgi.com/irix/>
- Correctif pour UnixWare 7.1.1, OpenUNIX 8.0.0 et UnixWare 7.1.3
<ftp://ftp.sco.com/pub/updates/OpenUNIX/CSSA-2003-SCO.1.1>

Gestion détaillée du document

28 février 2003 version initiale.