

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de linuxconf

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-2002-AVI-193>

Gestion du document

Référence	CERTA-2002-AVI-193-001
Titre	Vulnérabilité de linuxconf
Date de la première version	29 août 2002
Date de la dernière version	09 septembre 2002
Source(s)	Avis de sécurité "Linuxconf locally exploitable buffer overflow" de iDEFENSE
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

Linuxconf 1.28r3 et versions antérieures.

3 Résumé

Une vulnérabilité de type débordement de mémoire présente dans la commande linuxconf permet, sous certaines conditions, à un utilisateur mal intentionné de réaliser une élévation de privilèges.

4 Description

Linuxconf est un outil d'administration pour les plate-formes Linux.

Une vulnérabilité de type débordement de mémoire est présente dans la routine de traitement de la variable d'environnement `LINUXCONF_LANG`.

Si le drapeau `suid` est positionné sur l'exécutable `/bin/linuxconf`, cette vulnérabilité peut être exploitée par un utilisateur local afin de réaliser une élévation de privilèges.

5 Contournement provisoire

Retirer le drapeau `suid`:

```
chmod u-s /bin/linuxconf
```

6 Solution

La version 1.28r4 corrige la vulnérabilité :

<http://www.solucorp.qc.ca/linuxconf>

7 Documentation

– linuxconf 1.28r4 changes log :

<http://www.solucorp.qc.ca/changes hc?projet=linuxconf&version=1.28r4>

– Avis de sécurité "Linuxconf locally exploitable buffer overflow" de iDEFENSE :

<http://online.securityfocus.com/archive/1/289585/2002-08-26/2002-09-01/0>

– Avis de sécurité MDKSA-2002-56 de Mandrake :

<http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-056.php>

Gestion détaillée du document

29 août 2002 version initiale.

09 septembre 2002 Ajout de l'avis de sécurité de Mandrake.