



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 novembre 2003
N° CERTA-2003-AVI-196

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités sur HP-UX

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-196>

Gestion du document

Référence	CERTA-2003-AVI-196
Titre	Vulnérabilités sur HP-UX
Date de la première version	14 novembre 2003
Date de la dernière version	–
Source(s)	Avis de sécurité SA2003-07 de NSFOCUS Avis de sécurité SA2003-08 de NSFOCUS
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

- HP-UX B.11.00;
- HP-UX B.11.11.

La seconde vulnérabilité est également présente sur les systèmes suivants :

- HP-UX B.10.20;
- HP-UX B.11.22.

3 Résumé

Deux vulnérabilités présentes sur HP-UX permettent à un utilisateur mal intentionné ayant déjà un compte sur le système d'exécuter du code arbitraire avec les privilèges du super utilisateur (`root`).

4 Description

Un débordement de mémoire dans les programmes `setuid root` (`swinstall`, `swmodify`) du logiciel `Software Distributor` permet à un utilisateur mal intentionné du système d'exécuter du code arbitraire avec les privilèges du super utilisateur `root`.

Une vulnérabilité de type chaîne de format présente lors du traitement de la variable `NLSPATH` par des programmes `setuid root` permet à un utilisateur du système d'exécuter du code arbitraire avec les privilèges du super utilisateur `root`.

5 Solution

Appliquer les correctif disponibles sur le site HP (cf section documentation).

6 Documentation

Pour la première vulnérabilité :

- Avis de sécurité SA2003-07 de NSFOCUS :
<http://www.nsfocus.com/english/homepage/research/0307.htm>
- Avis de sécurité HP-UX :
<http://www1.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0311-293>
- Référence CVE de la première vulnérabilité : CAN-2003-0089
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0089>

Pour la seconde vulnérabilité :

- Avis de sécurité SA2003-08 de NSFOCUS :
<http://www.nsfocus.com/english/homepage/research/0308.htm>
- Avis de sécurité HP-UX :
<http://www1.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0311-294>
- Référence CVE de la seconde vulnérabilité : CAN-2003-0090 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0090>

Gestion détaillée du document

14 novembre 2003 version initiale.