



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 novembre 2000
N° CERTA-2000-AVI-073

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sous HP-UX du script auto_parms

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-2000-AVI-073>

Gestion du document

Référence	CERTA-2000-AVI-073
Titre	Vulnérabilité sous HP-UX du script auto_parms
Date de la première version	21 novembre 2000
Date de la dernière version	–
Source(s)	Bulletin de sécurité Hewlett Packard
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 en local aux privilèges administrateur ;
- Déni de service ;
- Risque important car l'exploitation de la vulnérabilité est facilement accessible.

2 Systèmes affectés

HP9000 séries 700/800 sous HP-UX 10.xx et 11.xx

3 Résumé

Deux vulnérabilités découvertes dans le script Auto_parms permettent à un utilisateur local d'usurper les privilèges root lors du démarrage de la machine.

4 Description

Le script Auto_parms permet de gérer la configuration DHCP (Dynamic Host Configuration Protocol). Ce script est appelé à chaque démarrage de la machine. Les vulnérabilités découvertes permettent à un utilisateur mal

intentionné d'usurper les privilèges de ROOT lors du lancement de ce script.

Un programme permettant de réaliser d'exploiter cette vulnérabilité est largement répandu sur internet.

5 Solution

Correctifs suivant les versions d'HP-UX :

Version	correctif
HP-UX 11.00	PHCO_21993
HP-UX 11.04	PHCO_22186
HP-UX 10.20	PHCO_21992
HP-UX 10.24	PHCO_22185
HP-UX 10.26	PHCO_22591
HP-UX 10.10	PHCO_21991
HP-UX 10.16	PHCO_22634
HP-UX 10.01	PHCO_21990

Correctif disponible sur le site :

<http://europe-support.external.hp.com>

6 Documentation

Bulletin de sécurité HP

<http://itrc.hp.com>

Gestion détaillée du document

21 novembre 2000 version initiale.