

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans 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-2009-AVI-292>

---

### Gestion du document

Référence	CERTA-2009-AVI-292-001
Titre	Vulnérabilités dans HP-UX
Date de la première version	27 juillet 2009
Date de la dernière version	26 mars 2010
Source(s)	Bulletin de sécurité HP #c01763606 du 21 juillet 2009
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 à distance ;
- déni de service à distance.

## 2 Systèmes affectés

- HP-UX 11.x.

## 3 Résumé

Deux vulnérabilités découvertes dans la mise en œuvre du service NTP dans HP-UX permettent à un utilisateur malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire à distance.

## 4 Description

Une vulnérabilité de type débordement de mémoire est présente dans la fonction `cookedprint()`. Elle peut être exploitée au moyen d'un paquet spécialement construit afin de provoquer un déni de service ou d'exécuter du code arbitraire.

Une seconde vulnérabilité de type débordement de mémoire présente dans la fonction `crypto_recv()` peut être exploitée à distance au moyen d'un paquet spécialement construit envoyé au démon `xntpd`.

## 5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité HP #c01763606 du 21 juillet 2009 :  
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document/.jsp?objectID=c01763606>
- Bulletin de sécurité HP #c01961959 du 23 mars 2010 :  
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document/.jsp?objectID=c01961959>
- Avis de sécurité CERTA-2009-AVI-195 du 19 mai 2009 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-195/CERTA-2009-AVI-195.html>
- Référence CVE CVE-2009-0159 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0159>
- Référence CVE CVE-2009-1252 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1252>

## Gestion détaillée du document

**27 juillet 2009** version initiale.

**26 mars 2010** ajout de la référence au bulletin de sécurité HP #01961959.