



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 octobre 2009
N° CERTA-2009-AVI-428

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Kerberos sous 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-428>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2009-AVI-428 |
| Titre | Multiples vulnérabilités dans Kerberos sous HP-UX |
| Date de la première version | 08 octobre 2009 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité HP c01717795 du 30 septembre 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

- Client Kerberos versions 1.3.5.09 et antérieures sous HP-UX B.11.11 ;
- client Kerberos versions 1.6.2 et antérieures sous HP-UX B.11.23 et HP B.11.31.

3 Résumé

Plusieurs vulnérabilités ont été corrigées dans les clients Kerberos fonctionnant sous HP-UX. Ces vulnérabilités permettent de provoquer un déni de service à distance ou d'exécuter du code arbitraire à distance.

4 Description

Deux vulnérabilités ont été identifiées dans les clients Kerberos fonctionnant sous HP-UX :

- la première concerne la fonction `asnl_decode_generaltime`. Un attaquant peut provoquer un déni

- de service distant ou exécuter du code arbitraire à distance par le biais d'un DER (Distinguished Encoding Rules) non valide ;
- la seconde concerne la fonction `asn1buf_imbed`. Un attaquant peut provoquer un déni de service distant par le biais d'une allocation mémoire particulière.

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 c01717795 du 30 septembre 2009 :
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01717795>
- Référence CVE CVE-2009-0846 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0846>
- Référence CVE CVE-2009-0847 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0847>

Gestion détaillée du document

08 octobre 2009 version initiale.