Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 janvier 2007
N° CERTA-2007-AVI-051

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Apache sur HP-UX

Gestion du document

Référence	CERTA-2007-AVI-051
Titre	Vulnérabilités dans Apache sur HP-UX
Date de la première version	25 janvier 2007
Date de la dernière version	–
Source(s)	Mise à jour d'Apache pour HP-UX
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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

HP-UX B.11.x exécutant des versions d'*Apache-based Web Server* antérieures à 2.0.58.01.

3 Résumé

Plusieurs vulnérabilités concernant *Apache* sur *HP-UX* permettraient à un attaquant d'exécuter du code arbitraire à distance, de provoquer un déni de service à distance et/ou de contourner la politique de sécurité.

4 Description

Plusieurs vulnérabilités sur les versions antérieures à 0.9.7l et 0.9.8d d'*OpenSSL* permettent à une personne malintentionnée d'exécuter du code arbitraire à distance, de provoquer un déni de service à distance, et/ou de contourner la politique de sécurité.

Ces vulnérabilités d'*OpenSSL* sont corrigées dans la mise à jour de *HP-UX Apache-based Web Server* 2.0.58.01. Une mise à jour est également disponible pour le logiciel *OpenSSL* sur *HP-UX* sans *Apache*.

5 Solution

Se référer aux mises à jour de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Mise à jour d'Apache pour HP-UX du 10 janvier 2007 :
  http://h20293.www2.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=HPUXWSSUITE

- Mise à jour d'OpenSSL pour HP-UX :
  http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=OPENSSL11I
- Référence CVE CVE-2006-2940 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2940
- Référence CVE CVE-2006-2937 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2937
- Référence CVE CVE-2006-3738 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3738
- Référence CVE CVE-2006-4343 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4343
- Référence CVE CVE-2006-4339 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4339
- Référence CVE CVE-2005-2969 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2969

Gestion détaillée du document

25 janvier 2007 version initiale.