Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 avril 2012
N° CERTA-2012-AVI-225

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnératilités dans HP-UX

Gestion du document

Référence	CERTA-2012-AVI-225
Titre	Multiples vulnérabilités dans HP-UX
Date de la première version	20 avril 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité HP-UX c03278391 du 18 avril 2012
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

- Déni de service à distance ;
- atteinte à l'intégrité des données ;
- élévation de privilèges.

2 Systèmes affectés

- HP-UX B.11.23 ;
- HP-UX B.11.31 ;
- HP-UX B.11.11.

3 Résumé

De multiples vulnérabilités ont été corrigées dans le module *Apache* de *HP-UX*. Elles permettent à un utilisateur malintentionné de porter atteinte à la confidentialité des données, causer un déni de service et d'élever ses privilèges. La liste ci-dessous fournit le détail de ces vulnérabilités :

- CVE-2011-3607 : la fonction *api_pregsub*, lorsque le module *mod_setenvif* est activé, est vulnérable à un dépassement d'entier permettant à un utilisateur malintentionné d'élever ses privilèges ;

- CVE-2012-0021 : *mod_log_config* ne gère pas correctement certains cookies, ce qui peut conduire à un arrêt inopiné du service Apache ;
- CVE-2012-0031 : un problème dans la gestion des segments de mémoire partagée peut conduire à un déni de service local ;
- CVE-2012-0053 : lorsqu'aucune page personnalisée n'est définie pour le code d'erreur 400, il est possible d'obtenir les cookies httpOnly.

4 Solution

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

5 Documentation

- Document du CERTA CERTA-2012-AVI-050 du 02 février 2012 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-050/index.html
- Bulletin de sécurité HP c03278391 du 18 avril 2012 :
  http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03278391
- Référence CVE CVE-2011-3607 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3607
- Référence CVE CVE-2012-0021 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0021
- Référence CVE CVE-2012-0031 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0031
- Référence CVE CVE-2012-0053 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0053

Gestion détaillée du document

20 avril 2012 version initiale.