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 2008
N° CERTA-2008-AVI-479-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Lighttpd

Gestion du document

Référence	CERTA-2008-AVI-479-001
Titre	Multiples vulnérabilités dans Lighttpd
Date de la première version	30 septembre 2008
Date de la dernière version	08 octobre 2008
Source(s)	Bulletins de sécurité Lighttpd 04, 05, 06 et 07
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 ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données .

2 Systèmes affectés

Toutes les versions de `Lighttpd` antérieures à la version 1.4.20.

3 Résumé

Plusieurs vulnérabilités dans `Lighttpd` peuvent être exploitées par une personne malveillante afin de provoquer un déni de service, de contourner la politique de sécurité ou d'accéder à des informations sensibles.

4 Description

Plusieurs vulnérabilités affectant `Lighttpd` ont été découvertes :

- une faiblesse dans la gestion de la mémoire par la fonction *http_request_parse()* permet à une personne malintentionnée d'obtenir un accès total à la mémoire ;
- une erreur dans la gestion des noms de fichier permet à une personne malintentionnée de poter atteinte à la confidentialité des données ;
- une erreur due au non décodage des requêtes avant le contrôle avec les règles de réécriture et de redirection permet à une personne malveillante de contourner ces dernières.

5 Solution

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

6 Documentation

- Bulletins de sécurité de Lighttpd :
  http://trac.lighttpd.net/security/lighttpd_sa_2008_05.txt
  http://trac.lighttpd.net/security/lighttpd_sa_2008_06.txt
  http://trac.lighttpd.net/security/lighttpd_sa_2008_07.txt
- Référence CVE CVE-2008-4298 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4298
- Référence CVE CVE-2008-4359 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4359
- Référence CVE CVE-2008-4360 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4360

Gestion détaillée du document

30 septembre 2008 version initiale.
08 octobre 2008 ajout de vulnérabilités et des références CVE.