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 août 2009
N° CERTA-2009-AVI-347

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans la bibliothèque neon

Gestion du document

Référence	CERTA-2009-AVI-347
Titre	Vulnérabilités dans la bibliothèque neon
Date de la première version	25 août 2009
Date de la dernière version	–
Source(s)	Annonce de la version 0.28.6 de neon du 18 août 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

- Déni de service à distance ;
- attaque de type homme-au-milieu.

2 Systèmes affectés

neon versions 0.28.5 et antérieures.

3 Résumé

Deux vulnérabilités dans *neon* permettent de réaliser des attaques de type homme-au-milieu ou un déni de service à distance.

4 Description

Deux vulnérabilités ont été découvertes dans *neon* :

- un déni service est possible, via des fichiers au format XML ou un serveur DAV malveillant, si la bibliothèque *expat* est utilisée (CVE-2009-2473) ;

– le mécanisme de vérification des certificats utilisés lors de sessions `SSL` peut être contourné, ce qui permet des attaques de type homme-au-milieu (CVE-2009-2474).

5 Solution

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

6 Documentation

– Annonce de la version 0.28.6 de neon du 18 août 2009 :
http://lists.manyfish.co.uk/pipermail/neon/2009-August/001044.html
– Descriptif des vulnérabilités corrigées :
http://lists.manyfish.co.uk/pipermail/neon/2009-August/001045.html
http://lists.manyfish.co.uk/pipermail/neon/2009-August/001046.html
– Référence CVE CVE-2009-2473 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2473
– Référence CVE CVE-2009-2474 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2474

Gestion détaillée du document

25 août 2009 version initiale.