Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 décembre 2010
N° CERTA-2010-AVI-579

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans AWStats

Gestion du document

Référence	CERTA-2010-AVI-579
Titre	Vulnérabilités dans AWStats
Date de la première version	06 décembre 2010
Date de la dernière version	–
Source(s)	Note de vulnérabilité de l'US-CERT VU#870532 du 30 novembre 2010
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.

2 Systèmes affectés

AWStats 6.95 et versions antérieures.

3 Résumé

Des vulnérabilités affectent AWStats dont certaines permettent à un utilisateur malveillant d'exécuter du code à distance.

4 Description

Des vulnérabilités affectent AWStats :

– l'acceptation par *awstat.cgi* d'un chemin vers un fichier de configuration dans l'adresse réticulaire (URL) permet à un utilisateur malveillant d'exécuter du code à distance au moyen d'un fichier de configuration malveillant dans un répertoire NFS ou WebDAV ;

- le même problème est également présent sous Windows avec les fichiers partagés ;
- l'utilisation de *LoadPlugin* permet à un utilisateur malveillant de parcourir une partie non autorisée de l'arborescence des fichiers.

5 Solution

La version 7.0 d'AWStats corrige ces problèmes.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site de téléchargement du projet AWStats :
  http://awstats.sourceforge.net
- Note de vulnérabilité de l'US-CERT VU#870532 du 30 novembre 2010 :
  http://www.kb.cert.org/vuls/id/870532
- Référence CVE CVE-2010-4367 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4367
- Référence CVE CVE-2010-4368 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4368
- Référence CVE CVE-2010-4369 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4369

Gestion détaillée du document

06 décembre 2010 version initiale.