Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 juin 2006
N° CERTA-2006-AVI-184-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de AWStats

Gestion du document

Référence	CERTA-2006-AVI-184-002
Titre	Vulnérabilité de AWStats
Date de la première version	05 mai 2006
Date de la dernière version	12 juin 2006
Source(s)	Bulletin de mise à jour de AWStats
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

Les versions 6.4 et 6.5 d'AWStats.

3 Résumé

Une vulnérabilité existe dans les versions 6.4 et 6.5 d'AWStats. Elle permet à une personne malveillante d'envoyer une requête particulière conduisant à l'exécution de code arbitraire à distance.

4 Description

AWStats est un outil d'analyse statistique pour site web. Les versions 6.4 et 6.5 présentent une vulnérabilité de la mise à jour des valeurs statistiques lançée à partir de la page web. La valeur d'entrée du paramètre `migrate` n'est pas suffisamment contrôlée. Un utilisateur peut alors envoyer une requête particulière qui ne sera pas correctement interprétée par la fonction Perl `open()`, afin d'injecter et d'exécuter des commandes à distance. Celles-ci

seront lancées avec les mêmes privilèges que le processus associé à l'interface `CGI` d'AWStats. Il faut noter que cette méthode est possible si l'option `AllowToUpdateStatsFromBrowser` est activée dans le fichier de configuration d'AWStats. Ce n'est pas le cas par défaut.

5 Solution

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

6 Documentation

- Mise à jour de l'outil AWStats :
  http://awstats.sourceforge.net
- Bulletin de sécurité FreeBSD du 05 mai 2006 :
  http://www.vuxml.org/freebsd/pkg-awstats.html
- Bulletin de sécurité Debian DSA-1058 du 18 mai 2006 :
  http://www.debian.org/security/2006/dsa-1058
- Bulletin de sécurité Gentoo GLSA 200606-06 du 07 juin 2006 :
  http://www.gentoo.org/security/en/glsa/glsa-200606-06.xml
- Référence CVE CVE-2006-2237 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2237

Gestion détaillée du document

05 mai 2006 version initiale.
19 mai 2006 ajout des références aux bulletins de sécurité FreeBSD, Debian et de la référence CVE.
12 juin 2006 ajout de la référence au bulletin de sécurité Gentoo.