Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 31 août 2005
N° CERTA-2005-AVI-307-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de AWStats

Gestion du document

Référence	CERTA-2005-AVI-307-003
Titre	Vulnérabilité de AWStats
Date de la première version	10 août 2005
Date de la dernière version	10 novembre 2005
Source(s)	Bulletin de sécurité iDEFENSE 08.09.05
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.

2 Systèmes affectés

`AWStats` versions 6.3 et antérieures.

3 Description

`AWStats` est un outil d'analyse de fichiers de journalisation et de génération de statistiques pour les serveurs web, FTP ou mail.
Une vérification insuffisante de la validité du champ *referrer* présent dans des requêtes `http` permet à un utilisateur distant mal intentionné, par le biais d'une requête `http` malicieusement construite enregistrée dans les fichiers de journalisation du serveur web, d'exécuter du code arbitraire sur le système effectuant l'analyse de ces même fichiers.

4 Solution

La version 6.4 de `AWStats` corrige le problème et est disponible à l'adresse :
http://awstats.sourceforge.net/#DOWNLOAD

5 Documentation

- Bulletin de sécurité iDEFENSE 08.09.05 du 9 août 2005 :
  http://www.idefense.com/application/poi/display?id=290&type=vulnerabilities
- Site de AWStats :
  http://awstats.sourceforge.net/
- Bulletin de sécurité Gentoo GLSA-200508-07 du 16 août 2005 :
  http://security.gentoo.org/glsa/glsa-200508-07.xml
- Bulletin de sécurité SuSE du 19 août 2005 :
  http://www.novell.com/linux/security/advisories/2005_19_sr.html
- Bulletin de sécurité FreeBSD :
  http://www.vuxml.org/freebsd/pkg-awstats.html
- Bulletin de sécurité Debian dsa-892 du 10 novembre 2005 :
  http://www.debian.org/security/2005/dsa-892
- Référence CVE CAN-2005-1527 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1527

Gestion détaillée du document

10 août 2005 version initiale.
18 août 2005 ajout du bulletin de sécurité FreeBSD.
31 août 2005 ajout du bulletin de sécurité Gentoo et SuSE.
10 novembre 2005 ajout du bulletin de sécurité Debian.