

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de AWStats

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-035>

Gestion du document

Référence	CERTA-2005-AVI-035-003
Titre	Vulnérabilité de AWStats
Date de la première version	27 janvier 2005
Date de la dernière version	18 février 2005
Source(s)	Bulletin de sécurité iDEFENSE 01.17.05
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 à distance.

2 Systèmes affectés

Toutes les versions de AWStats antérieures à la version 6.3.

3 Description

AWStats est un outil d'analyse de fichiers journaux et de génération de statistiques pour les serveurs web, FTP ou mail.

Une vulnérabilité dans la validation des paramètres passés au script `awstats.pl` permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance avec les droits du serveur web.

4 Solution

Mettre à jour AWStats en version de développement 6.3 ou désactiver l'utilisation de AWStats en attendant la prochaine version stable 6.3 (cf. section Documentation).

5 Documentation

- Site Internet de AWStats :
<http://awstats.sourceforge.net>
- Fichier de la liste des changements de AWStats :
http://awstats.sourceforge.net/docs/awstats_changelog.txt
- Bulletin de sécurité iDEFENSE 01.17.05 du 17 janvier 2005 :
<http://www.idefense.com/application/poi/display?id=185&type=vulnerabilities>
- Bulletin de sécurité Gentoo GLSA 200501-36 du 25 janvier 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200501-36.xml>
- Bulletin de sécurité Debian DSA-682 du 15 février 2005 :
<http://www.debian.org/security/2005/dsa-682>
- Mise à jour de sécurité du paquetage NetBSD awstats :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/www/awstats/README.html>
- Bulletin de sécurité FreeBSD pour awstats du 16 février 2005 :
<http://www.vuxml.org/freebsd/>
- Référence CVE CAN-2005-0116 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0116>
- Référence CVE CAN-2005-0363 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0363>

Gestion détaillée du document

27 janvier 2005 version initiale.

15 février 2005 ajout de la référence au bulletin de sécurité Debian DSA-682 et des références CVE CAN-2005-0116 et CAN-2005-0363.

15 février 2005 ajout de la référence au bulletin de sécurité NetBSD.

18 février 2005 ajout de la référence au bulletin de sécurité FreeBSD.