Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 octobre 2001
N° CERTA-2001-AVI-132

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de webalizer

Gestion du document

Référence	CERTA-2001-AVI-132
Titre	Vulnérabilités de webalizer
Date de la première version	26 octobre 2001
Date de la dernière version	–
Source(s)	–
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

Webalizer versions 2.01-06 et antérieures.

3 Résumé

Deux vulnérabilités du programme webalizer permettent à un utilisateur mal intentionné d'inclure des scripts dans les rapports HTML générés par webalizer.

4 Description

Webalizer est un programme permettant de traiter les fichiers de logs d'un serveur HTTP. La nature de certains champs des fichiers de logs n'est pas vérifiée par le programme, et sont intégralement retranscrits dans le rapport généré en HTML.

Un utilisateur mal intentionné peut y inclure des scripts, qui seront exécutés soit par un navigateur parcourant ce rapport, soit par d'autres programmes qui interprètent ces rapports.

Les deux champs vulnérables sont :

- le nom de la machine accèdant au serveur HTTP ;
- le champ *Referer*.

5 Contournement provisoire

Si la résolution DNS est activée dans webalizer (option *–enable-dns*), s'assurer que le système de résolution DNS inverse filtre les méta-caractères HTML.

Modifier la configuration de webalizer pour qu'il ne traite plus le champ *Referer* des fichiers de logs (ce champ est traité dans la configuration par défaut).

6 Solution

Télécharger le correctif :
ftp://ftp.mrunix.net/pub/webalizer/sec-fix.patch

ou mettre à jour webalizer à la version 2.01-09.

Gestion détaillée du document

26 octobre 2001 version initiale.