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 octobre 2001
N° CERTA-2001-AVI-114

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le moteur d'indexation ht://Dig

Gestion du document

Référence	CERTA-2001-AVI-114
Titre	Vulnérabilité dans le moteur d'indexation ht://Dig
Date de la première version	12 octobre 2001
Date de la dernière version	–
Source(s)	Avis de sécurité Caldera
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

- Déni de service ;
- récupération d'informations.

2 Systèmes affectés

Toutes les versions de ht://Dig de 3.1.0 à 3.1.5.

3 Résumé

Un utilisateur mal intentionné peut, en exploitant une faille du script CGI htsearch, réaliser un déni de service et récupérer des informations sur le système.

4 Description

Le moteur d'indexation ht://Dig se compose de plusieurs outils, dont le programme `htsearch`, utilisé pour effectuer les recherches sur la base d'indexation.

Ce script peut être lancé soit comme CGI, soit par ligne de commande, qui accepte alors l'option `-c [nom_de_fichier]`. Cette option permet de lire un fichier de configuration particulier.

Le script CGI n'effectuant aucun filtrage pour l'empêcher d'utiliser des arguments de ligne de commande, un utilisateur distant peut alors utiliser l'option -c pour lire des fichiers sur le système et, dans certains cas, réaliser un déni de service.

5 Solution

Appliquer les correctifs de sécurité.

6 Documentation

Avis de sécurité Caldera :
http://caldera.com/support/security/advisories/CSSA-2001-035.0.txt

Gestion détaillée du document

12 octobre 2001 version initiale.