Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 octobre 2001
N° CERTA-2001-AVI-113

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans PhpNuke

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-2001-AVI-113

Gestion du document

Référence	CERTA-2001-AVI-113
Titre	Vulnérabilité dans PhpNuke
Date de la première version	08 octobre 2001
Date de la dernière version	–
Source(s)	Liste de diffusion BugTraq
Pièce(s) jointe(s)	Aucune

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Exécution de code à distance avec les privilèges de l'utilisateur d'Apache ;
- altération des données du portail.

Des exploits sont publiés.

2 Systèmes affectés

Toute version de PhpNuke jusqu'à la 5.2 comprise sur système d'exploitation Unix/Linux, OS/2, Windows, MacOS et FreeBSD.

3 Résumé

PhpNuke est un kit de création et gestion d'un portail internet/intranet s'appuyant sur un serveur Web Apache, le langage de pages "web" dynamiques Php et le gestionnaire de base de données MySQL.

Il est possible d'exécuter du code malicieux sur le serveur ou de lire le contenu d'un certain nombre de fichiers (dont le fichier de mots de passe de MySQL).

4 Description

Un script mal sécurisé permet à un utilisateur mal intentionné de télécharger et d'exécuter sur le serveur n'importe quel programme ou de lire tout fichier accessible au script.

Combiné avec un exploit local, cette faille permet d'obtenir les droits d'administrateur sur le serveur.

5 Contournement provisoire

Désactiver la fonction de téléchargement sur le serveur.

6 Solution

- Modifier le fichier *admin.php* comme suggéré à l'adresse suivante :
  http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=solution&id=3361
- Télécharger et installer le port/paquetage correspondant à la distribution lorsqu'il sera disponible.

7 Documentation

PhpNuke Remote File Copy Vulnerability
http://www.securityfocus.com/bid/3361

Gestion détaillée du document

08 octobre 2001 version initiale.