

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités du service ISC DHCP

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-2004-AVI-204>

Gestion du document

Référence	CERTA-2004-AVI-204-002
Titre	Multiples vulnérabilités du service ISC DHCP
Date de la première version	23 juin 2004
Date de la dernière version	29 juin 2004
Source(s) Avis de sécurité TA04-174A de l'US-CERT	
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 ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

ISC DHCP versions 3.0.1rc12 et 3.0.1rc13.

3 Résumé

De multiples vulnérabilités présentes dans le serveur ISC DHCP peuvent être exploitées, à distance, par un utilisateur mal intentionné afin d'exécuter du code arbitraire sur la plate-forme vulnérable.

4 Description

DHCP (Dynamic Host Configuration Protocol) est un protocole client-serveur décrit dans le RFC 2131. Le serveur fournit dynamiquement des adresses IP et autres paramètres de configuration réseau à des machines clientes.

Plusieurs vulnérabilités de type débordement de mémoire sont présentes dans le serveur ISC DHCP. Au moyen de paquets malicieusement constitués, un utilisateur mal intentionné peut exploiter ces vulnérabilités afin d'exécuter du code arbitraire sur la plate-forme vulnérable ou réaliser un déni de service par arrêt brutal du serveur.

5 Solution

La version 3.0.1rc14, disponible sur le site d'ISC, corrige cette vulnérabilité.

6 Documentation

- Internet Software Consortium (ISC) :
<http://www.isc.org/sw/dhcp>
- Avis de sécurité TA04-174A de l'US-CERT :
<http://www.us-cert.gov/cas/techalerts/TA04-174A.html>
- Bulletin de sécurité MDKSA-2004:061 de Mandrake du 22 juin 2004 :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:061>
- Bulletin de sécurité SuSE-SA:2004:0019 de SuSE du 22 juin 2004 :
http://www.suse.com/de/security/2004_19_dhcp_server.html
- Bulletin de sécurité FreeBSD pour isc-dhcp3-server du 25 juin 2004 :
<http://www.vuxml.org/freebsd/>
- Référence CVE CAN-2004-0460 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0460>
- Référence CVE CAN-2004-0461 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0461>

Gestion détaillée du document

23 juin 2004 version initiale.

24 juin 2004 ajout référence au bulletin de sécurité de SuSE.

29 juin 2004 ajout référence au bulletin de sécurité de FreeBSD.