

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du service ISC DHCPD

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-2002-AVI-108>

Gestion du document

Référence	CERTA-2002-AVI-108-001
Titre	Vulnérabilité du service ISC DHCPD
Date de la première version	23 mai 2002
Date de la dernière version	31 mai 2002
Source(s)	Avis CA-2002-12 du CERT/CC
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

Elévation de privilèges.

2 Systèmes affectés

ISC DHCPD versions 3.0 à 3.0.1rc8.

3 Résumé

ISC DHCPD est un logiciel libre mis à disposition par l'Internet Software Consortium.

DHCP (Dynamic Host Configuration Protocol) est basé sur un modèle client-serveur dans lequel un serveur DHCP fournit dynamiquement des adresses IP et autres paramètres de configuration à des machines clientes. DHCP s'appuie sur le protocole BOOTP (BOOTstrap Protocol).

Une vulnérabilité présente dans le traitement des requêtes de mise à jour DNS (`dns-update`) permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance sur le serveur DHCP avec les privilèges de l'administrateur système (`root`).

4 Description

Le serveur ISC DHCPD enregistre le résultat des requêtes de type `dns-update` destinées au serveur DNS. Une vulnérabilité de type chaîne de format présente dans la routine de traitement de ces requêtes permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance sur le serveur DHCP avec les privilèges de l'administrateur système (`root`).

La vulnérabilité n'est exploitable que si ISC DHCPD est compilé avec l'option `NSUPDATE` (configuration par défaut).

5 Contournement provisoire

Mettre en place un filtrage au niveau du garde-barrières sur les ports suivants, afin d'empêcher l'exploitation de cette vulnérabilité depuis l'Internet :

- 67/TCP (Bootstrap Protocol Server)
- 67/UDP (Bootstrap Protocol Server)
- 68/TCP (Bootstrap Protocol Client)
- 68/UDP (Bootstrap Protocol Client)

6 Solution

La version 3.0.1rc9 d'ISC DHCPD corrige cette vulnérabilité.

7 Documentation

- RFC 2131 "Dynamic Host Configuration Protocol" :
<ftp://ftp.isi.edu/in-notes/rfc2131.txt>
- Internet Software Consortium :
<http://www.isc.org>
- Avis de sécurité CA-2002-12 du CERT/CC :
<http://www.cert.org/advisories/CA-2002-12.html>
- Avis de sécurité NGSEC-2002-2 de Next Generation Security Technologies :
<http://www.ngsec.com/docs/advisories/NGSEC-2002-2.txt>
- Avis de sécurité SuSE-SA:2002:019 de SuSE :
http://www.suse.com/de/support/security/2002_19_dhcp.html
- Avis de sécurité MDKSA-2002:037 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-037.php>
- Avis de sécurité MDKSA-2002:037-1 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-037-1.php>

Gestion détaillée du document

23 mai 2002 version initiale.

31 mai 2002 Ajout lien sur l'avis SuSE et ajout références aux avis Mandrake.