



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 janvier 2003
N° CERTA-2003-AVI-005-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 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-2003-AVI-005>

Gestion du document

Référence	CERTA-2003-AVI-005-002
Titre	Vulnérabilité dans ISC DHCPD
Date de la première version	16 janvier 2003
Date de la dernière version	21 janvier 2003
Source(s)	Avis CA-2003-001 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

Exécution de code arbitraire à distance.

2 Systèmes affectés

ISC DHCPD versions 3.0 à 3.0.1RC10.

3 Résumé

ISC DHCPD est une implémentation de DHCP (Dynamic Host Configuration Protocol) fournie par l'Internet Software Consortium, et conforme à la RFC 2131.

Plusieurs vulnérabilités sont présentes dans ISC DHCP.

4 Description

ISC DHCPD possède une option NSUPDATE permettant la mise à jour automatique d'un serveur DNS.

Plusieurs vulnérabilités présentes dans NSUPDATE utilisé lors de la résolution de noms DNS, permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance par l'envoi d'un message DHCP astucieusement constitué.

5 Contournement provisoire

Mettre en place un filtrage au niveau du garde-barrière 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

Appliquer les correctifs ou mettre à jour par les versions 3.0p12 et 3.0.1RC11 corrigeant ces vulnérabilités.

7 Documentation

- Bulletin de sécurité CA-2003-001 du CERT/CC :
<http://www.cert.org/advisories/CA-2003-01.html>
- Bulletin de sécurité RHSA-2003:011-07 de RedHat :
<https://rhn.redhat.com/errata/RHSA-2003-011.html>
- Bulletin de sécurité DSA-231 de Debian :
<http://www.debian.org/security/2003/dsa-231>
- Bulletin de sécurité MDKSA-2003:007 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:007>
- Bulletin de sécurité SuSE-SA:2003:0006 de SuSE :
http://www.suse.com/de/security/2003_006_dhcp.html

Gestion détaillée du document

16 janvier 2003 version initiale.

17 janvier 2003 ajout du bulletin de RedHat.

21 janvier 2003 ajout références aux bulletins de Debian, Mandrake et Suse.