



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 juillet 2009
N° CERTA-2009-AVI-280

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans DHCP Dhclient

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-2009-AVI-280>

Gestion du document

Référence	CERTA-2009-AVI-280
Titre	Vulnérabilité dans DHCP Dhclient
Date de la première version	16 juillet 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité ISC du 14 juillet 2009
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 ;
- déni de service à distance.

2 Systèmes affectés

- dhcp 2.0 ;
- dhcp 3.0 ;
- dhcp 3.1 ;
- dhcp 4.0 ;
- dhcp 4.1.

3 Résumé

Une vulnérabilité présente dans la partie cliente de DHCP permet à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

Une vulnérabilité est présente dans la partie cliente de DHCP : `Dhclient`. Celle-ci est relative à la fonction `Script_write_params()`. Elle permet à un utilisateur distant malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire sur le système vulnérable par le biais d'un serveur DHCP construit de façon particulière.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité de l'ISC du 14 juillet 2009 :
<https://www.isc.org/node/468>
- Bulletin de sécurité Debian DSA 1833 du 14 juillet 2009 :
<http://www.debian.org/security/2009/dsa-1833>
- Note de vulnérabilité de l'US-CERT VU#410676 du 14 juillet 2009 :
<http://www.kb.cert.org/vuls/id/410676>
- Bulletin de sécurité Ubuntu USN-803-1 du 14 juillet 2009 :
<http://www.ubuntu.com/usn/usn-803-1>
- Référence CVE CVE-2009-0692 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0692>

Gestion détaillée du document

16 juillet 2009 version initiale.