



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 avril 2011
N° CERTA-2011-AVI-190-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le client DHCP ISC

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-2011-AVI-190>

Gestion du document

Référence	CERTA-2011-AVI-190-002
Titre	Vulnérabilité dans le client DHCP ISC
Date de la première version	06 avril 2011
Date de la dernière version	27 avril 2011
Source	Bulletin de l'ISC CVE-2011-0997 du 05 avril 2011
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

- DHCP versions 4.2.x antérieures à 4.2.1-P1 ;
- DHCP versions 4.1.x antérieures à 4.1.ESV-R2 ;
- DHCP versions 3.1.x antérieures à 3.1.ESV-R1.

3 Résumé

Une vulnérabilité dans le logiciel libre DHCP développé par l'Internet System Consortium permet à un attaquant d'exécuter du code arbitraire à distance.

4 Description

Le logiciel libre DHCP développé par l'Internet System Consortium ne vérifie pas la présence de certains caractères dans les réponses DHCP avant de les transmettre à un script. Il est donc possible, selon le script et le système d'exploitation cible, d'exécuter des commandes avec une réponse DHCP spécialement conçue.

5 Solution

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

6 Documentation

- Bulletin de l'ISC CVE-2011-0997 du 05 avril 2011 :
<https://www.isc.org/software/dhcp/advisories/cve-2011-0997>
- Bulletins de sécurité Debian DSA-2216 et 2217 du 10 avril 2011 :
<http://www.debian.org/security/2011/dsa-2216>
<http://www.debian.org/security/2011/dsa-2217>
- Bulletin de sécurité Fedora FEDORA-2011-4897 du 06 avril 2011 :
<http://lists.fedoraproject.org/pipermail/package-announce/2011-April/057888.html>
- Bulletin de sécurité Fedora FEDORA-2011-4935 du 07 avril 2011 :
<http://lists.fedoraproject.org/pipermail/package-announce/2011-April/058279.html>
- Bulletin de sécurité Mandriva MDVSA-2011:073 du 11 avril 2011 :
<http://www.mandriva.com/fr/support/security/advisories?name=MDVSA-2011:073>
- Bulletin de sécurité NetBSD NetBSD-SA2011-005 du 26 avril 2011 :
<http://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2011-005.txt.asc>
- Bulletin de sécurité Novell :
<http://support.novell.com/security/cve/CVE-2011-0997.html>
- Bulletin de sécurité Red Hat du 05 avril 2011 :
<https://www.redhat.com/security/data/cve/CVE-2011-0997.html>
- Bulletin de sécurité Ubuntu USN-1108-1 du 11 avril 2011 :
<http://www.ubuntu.com/usn/USN-1108-1/>
- Référence CVE CVE-2011-0997 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0997>

Gestion détaillée du document

06 avril 2011 version initiale.

11 avril 2011 ajout des bulletins de sécurité Red Hat et Novell.

27 avril 2011 ajout des bulletins de sécurité Debian, Fedora, Mandriva, NetBSD et Ubuntu.