

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du traitement DHCP par Windows Vista

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-2008-AVI-080>

Gestion du document

Référence	CERTA-2008-AVI-080
Titre	Vulnérabilité du traitement DHCP par Windows Vista
Date de la première version	13 février 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-004 du 12 février 2008
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

- Dénis de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Windows Vista ;
- Windows Vista Edition x64.

3 Résumé

Une vulnérabilité a été identifiée dans le traitement de réponses DHCP par le système Microsoft Windows Vista. Elle pourrait être exploitée par une personne malveillante afin de perturber les couches protocolaires et éventuellement redémarrer le système.

4 Description

Une vulnérabilité a été identifiée dans le traitement de réponses DHCP par le système Microsoft Windows Vista. DHCP, ou *Dynamic Host Configuration Protocol*, est le protocole utilisé par différents éléments réseau afin d'obtenir les informations nécessaires à leur fonctionnement (adresse IP disponible, adresse des serveurs DNS et passerelles associées, etc.).

Le système d'exploitation ne gère pas correctement certaines réponses retournées par un serveur DHCP. Une personne malveillante pourrait ainsi forger de telles réponses afin de perturber les couches protocolaires et éventuellement forcer les systèmes en attente de réponse à redémarrer.

5 Solution

Se référer au bulletin de sécurité MS08-004 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS08-004 du 12 février 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-004.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS08-004.msp>
- Référence CVE CVE-2008-0084 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0084>

Gestion détaillée du document

13 février 2008 version initiale.