

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités des pilotes Microsoft pour Intel Centrino PRO/Wireless

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-2006-AVI-316>

Gestion du document

Référence	CERTA-2006-AVI-316
Titre	Multiples vulnérabilités des pilotes Microsoft pour Intel Centrino PRO/Wireless
Date de la première version	02 août 2006
Date de la dernière version	–
Source(s)	Bulletins de sécurité Intel du 28 juillet 2006
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 ;
- contournement de la politique de sécurité ;
- élévation de privilèges.

2 Systèmes affectés

- Les pilotes Intel Pro/Wireless 2100 Network Connection de version antérieure à 7.1.4.6.
- Les pilotes Intel Pro/Wireless 2200BG Network Connection de version antérieure à 10.5.
- Les pilotes Intel Pro/Wireless 2915ABG Network Connection de version antérieure à 10.5.
- Les pilotes Intel Pro/Wireless 3945ABG Network Connection de version antérieure à 10.5.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans les pilotes Microsoft de certains matériels Intel pour les connexions sans-fil. Elles permettraient à une personne malveillante d'élever ses privilèges à ceux d'administrateur, d'obtenir des informations sur la sécurité du réseau sans-fil ou d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités ont été identifiées dans les pilotes Microsoft de certains matériels Intel pour les connexions sans-fil. Ceux-ci font partie de la technologie mobile Intel Centrino et peuvent être intégrés dans des ordinateurs portables ou tout autre appareil communiquant en Wi-Fi 802.11b/g et éventuellement 802.11a (pour le matériel Intel Pro/Wireless 3945ABG). Ils se présentent sous la forme de cartes au format MiniPCI.

Parmi ces vulnérabilités :

- Certaines permettent à un utilisateur malveillant distant, via un réseau sans-fil, d'envoyer des paquets mal interprétés par le pilote. Sous certaines conditions, la corruption de mémoire engendrée peut alors entraîner l'exécution de code arbitraire avec les droits de l'administrateur.
- L'une d'elles est due à un usage non maîtrisé de la mémoire partagée. Elle peut être exploitée par un utilisateur (ou une application) local du système vulnérable, afin d'obtenir des informations confidentielles sur la sécurité du réseau Wi-Fi : cela peut être la clé partagée WEP, ou les diverses informations d'authentification.
- L'une d'elles serait due à une vérification non correcte des requêtes d'accès par certains pilotes de plus haut niveau ou applicatifs. L'injection de paquets malformés destinés à une application particulièrement conçue permettrait à un utilisateur d'élever ces privilèges à ceux d'administrateur.

5 Solution

Se référer aux bulletins de sécurité de l'éditeur Intel pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Intel CS-023068 du 28 juillet 2006 :
<http://support.intel.com/support/wireless/wlan/sb/CS-023068.htm>
- Bulletin de sécurité Intel CS-023065 du 28 juillet 2006 :
<http://support.intel.com/support/wireless/wlan/sb/CS-023065.htm>
- Bulletin de sécurité Intel CS-023066 du 28 juillet 2006 :
<http://support.intel.com/support/wireless/wlan/sb/CS-023066.htm>
- Bulletin de sécurité Intel CS-023067 du 28 juillet 2006 :
<http://support.intel.com/support/wireless/wlan/sb/CS-023067.htm>
- Référence CVE CVE-2006-2316 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2316>

Gestion détaillée du document

02 août 2006 version initiale.