

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du protocole IPv6 dans le noyau Linux

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-2007-AVI-120>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2007-AVI-120 |
| Titre | Vulnérabilité du protocole IPv6 dans le noyau Linux |
| Date de la première version | 13 mars 2007 |
| Date de la dernière version | – |
| Source(s) | Changements du noyau Linux 2.6.20.2 du 09 mars 2007 |
| 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

- Contournement de la politique de sécurité ;
- Elévation de privilèges ;
- déni de service.

2 Systèmes affectés

Les noyaux Linux disposant d'une pile protocolaire IPv6 et de version antérieure à la 2.6.20.2

3 Description

Une vulnérabilité a été identifiée dans la mise en œuvre du protocole IPv6 pour les noyaux Linux. Elle impliquerait la fonction `ipv6_getsockopt_sticky` et permettrait à une personne locale au système d'accéder, de manière illégitime, à une partie de la mémoire.

4 Solution

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

5 Documentation

- CVE CVE-2007-1000 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1000>
- Changements du noyau Linux 2.6.20.2 du 09 mars 2007 :
<http://www.kernel.org/pub/linux/kernel/v2.6/Changelog-2.6.20.2>

Gestion détaillée du document

13 mars 2007 version initiale.