

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du 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-2009-AVI-337>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2009-AVI-337-003 |
| Titre | Vulnérabilité du noyau Linux |
| Date de la première version | 14 août 2009 |
| Date de la dernière version | 21 août 2009 |
| Source(s) | Bulletin d'annonce d'erreur RedHat 516949 du 14 août 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

Élévation de privilèges.

2 Systèmes affectés

- Les noyaux Linux 2.4.37.4 et antérieurs ;
- les noyaux 2.6.30.4 et antérieurs.

3 Résumé

Une vulnérabilité affectant les noyaux Linux et permettant une élévation de privilèges a été corrigée.

4 Description

Une vulnérabilité récente affectant les noyaux Linux a été rendue publique. Elle concerne un déréférencement de pointeur NULL à la création de *sockets* pour quelques protocoles et permet l'élévation de privilèges.

5 Solution

Le correctif actuel se trouve dans le `Git` de *kernel.org* mais devrait être rapidement intégré dans les différentes distributions. (cf. section Documentation).

6 Documentation

- Soumission du 13 août 2009 dans le `Git` de *kernel.org* :
<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=e694958388c50148389b0e9b9e9e8945cf0f1b98>
- Article de l'ISC SANS 6964 du 14 août 2009 :
<http://isc.sans.org/diary.html?storyid=6964>
- Bulletins d'annonce d'erreur RedHat 516949 du 14 août 2009 :
https://bugzilla.redhat.com/show_bug.cgi?id=516949
https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2009-2692
- Bulletins de sécurité Debian DSA-1862 du 14 août 2009 et DSA-1864 du 16 août 2009 :
<http://www.us.debian.org/security/2009/dsa-1862>
<http://www.us.debian.org/security/2009/dsa-1864>
- Bulletins de sécurité Fedora 10 et 11 du 15 août 2009 :
<https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00727.html>
<https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00728.html>
- Bulletin de sécurité Mandriva MDVSA-2009:205 du 17 août 2009 :
<http://www.mandriva.com/en/security/advisories?name=MDVSA-2009:205>
- Bulletin de sécurité Suse SUSE-SA:2009:045 du 20 août 2009 :
<http://lists.opensuse.org/opensuse-security-announce/2009-08/msg00007.html>
- Bulletin de sécurité Ubuntu USN-819-1 du 19 août 2009 :
<http://www.ubuntu.com/usn/usn-819-1>
- Référence CVE CVE-2009-2692 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2692>

Gestion détaillée du document

14 août 2009 version initiale.

18 août 2009 ajout des références aux bulletins de sécurité Mandriva, Fedora et Debian.

19 août 2009 correction de coquille et ajout de la référence au bulletin de sécurité Ubuntu.

21 août 2009 ajout de la référence au bulletin de sécurité Suse.