Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 mai 2013
N° CERTA-2013-ALE-005-002

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans le noyau Linux

Gestion du document

Référence	CERTA-2013-ALE-005-002
Titre	Vulnérabilité dans le noyau Linux
Date de la première version	14 mai 2013
Date de la dernière version	24 mai 2013
Source(s)	Correctif de sécurité du noyau Linux du 13 avril 2013
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(s)

– élévation de privilèges.

2 Systèmes affectés

– Noyau Linux de la version 2.6.37 à la version 3.8.8 ;
– Debian version stable (Wheezy) ;
– CentOS version stable (6.4) avec un noyau 2.6.32 qui intègre la fonctionnalité ;
– Toutes les autres distributions sont probablement vulnérables si elles utilisent un noyau concerné.

Les noyaux Linux versions supérieures à 3.8.8 et inférieures à 2.6.37 ne semblent pas être affectés, ainsi que les dernières versions stables supportées par le noyau Linux :
– Noyau Linux version 3.4.45
– Noyau Linux version 3.2.45
– Noyau Linux version 3.0.78

3 Résumé

Une vulnérabilité a été corrigée dans *le noyau Linux*. Elle permet à un attaquant de provoquer une élévation de privilèges. Un code d'exploitation est disponible publiquement et activement utilisé.

4 Contournement provisoire

En attendant que votre distribution intègre le correctif, il est possible de contourner le code d'exploitation en utilisant un noyau durci tel que *grsecurity* ou les fonctionnalités processeurs :

- *Supervisor Mode Access Prevention* ;
- *Supervisor Mode Execution Protection*.

Il est aussi possible de :

- recompiler son noyau avec le correctif du noyau Linux ;
- recompiler son noyau en désactivant la fonctionnalité *CONFIG_PERF_EVENTS* ;
- d'utiliser un noyau *vanilla* stable corrigé.

5 Solution

Installer les derniers correctifs de votre distribution Linux :

- Debian : DSA-2669-1
- Ubuntu LTS : USN-1825-1, USN-1828-1
- Red Hat : RHSA-2013-0830, RHSA-2013-0832, RHSA-2013-0829, RHSA-2013-0840, RHSA-2013-0841
- SUSE Linux Enterprise : SUSE-SU-2013:0819-1

Mandriva n'a pas encore corrigé la vulnérabilité.

6 Documentation

- Bulletin de sécurité Debian DSA-2669-1 du 15 mai 2013 :
  http://www.debian.org/security/2013/dsa-2669
- Bulletin de sécurité Ubuntu USN-1828-1 du 15 mai 2013 :
  http://www.ubuntu.com/usn/usn-1828-1/
- Bulletin de sécurité Ubuntu USN-1825-1 du 15 mai 2013 :
  http://www.ubuntu.com/usn/usn-1825-1/
- Bulletin de sécurité Red Hat RHSA-2013-0830 du 16 mai 2013 :
  https://rhn.redhat.com/errata/RHSA-2013-0830.html
- Bulletin de sécurité Red Hat RHSA-2013-0832 du 17 mai 2013 :
  https://rhn.redhat.com/errata/RHSA-2013-0832.html
- Bulletin de sécurité Red Hat RHSA-2013-0829 du 20 mai 2013 :
  https://rhn.redhat.com/errata/RHSA-2013-0829.html
- Bulletin de sécurité Red Hat RHSA-2013-0840 du 20 mai 2013 :
  https://rhn.redhat.com/errata/RHSA-2013-0840.html
- Bulletin de sécurité Red Hat RHSA-2013-0841 du 20 mai 2013 :
  https://rhn.redhat.com/errata/RHSA-2013-0841.html
- Bulletin de sécurité SUSE SUSE-SU-2013:0819-1 du 22 mai 2013 :
  https://www.suse.com/support/update/announcement/2013/suse-su-20130819-1.html
- Correctif de sécurité du noyau Linux du 13 avril 2013 :
  https://patchwork.kernel.org/patch/2441281/
- Référence CVE CVE-2013-2094 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2094

Gestion détaillée du document

14 mai 2013 version initiale.
22 mai 2013 ajout correctifs éditeurs.
24 mai 2013 ajout correctif SUSE.