



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 juillet 2013
N° CERTA-2013-AVI-411

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans le noyau Linux de SUSE

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-2013-AVI-411>

Gestion du document

Référence	CERTA-2013-AVI-411
Titre	Multiples vulnérabilités dans le noyau Linux de SUSE
Date de la première version	15 juillet 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité SUSE SUSE-SU-2013:1182-2 du 12 juillet 2013 Bulletin de sécurité SUSE SUSE-SU-2013:1151-1 du 12 juillet 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)

- exécution de code arbitraire
- déni de service
- atteinte à la confidentialité des données
- élévation de privilèges

2 Systèmes affectés

- SUSE version Linux Enterprise Server 11 SP3
- SUSE version Linux Enterprise High Availability Extension 11 SP3
- SUSE version Linux Enterprise Desktop 11 SP3
- SUSE version Linux Enterprise Desktop 11 SP2
- SUSE version Linux Enterprise High Availability Extension 11 SP2
- SUSE version Linux Enterprise Server 11 SP2

3 Résumé

De multiples vulnérabilités ont été corrigées dans le noyau Linux de *SUSE*. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, un déni de service et une atteinte à la confidentialité des données.

4 Solution

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

5 Documentation

- Bulletin de sécurité SUSE SUSE-SU-2013:1182-2 du 12 juillet 2013
<https://www.suse.com/support/update/announcement/2013/suse-su-20131182-2.html>
- Bulletin de sécurité SUSE SUSE-SU-2013:1151-1 du 12 juillet 2013
<https://www.suse.com/support/update/announcement/2013/suse-su-20131151-1.html>
- Référence CVE CVE-2013-0160
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0160>
- Référence CVE CVE-2013-1774
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1774>
- Référence CVE CVE-2013-1979
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1979>
- Référence CVE CVE-2013-3076
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3076>
- Référence CVE CVE-2013-3222
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3222>
- Référence CVE CVE-2013-3223
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3223>
- Référence CVE CVE-2013-3224
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3224>
- Référence CVE CVE-2013-3225
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3225>
- Référence CVE CVE-2013-3227
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3227>
- Référence CVE CVE-2013-3228
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3228>
- Référence CVE CVE-2013-3229
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3229>
- Référence CVE CVE-2013-3231
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3231>
- Référence CVE CVE-2013-3232
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3232>
- Référence CVE CVE-2013-3234
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3234>
- Référence CVE CVE-2013-3235
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3235>

Gestion détaillée du document

15 juillet 2013 version initiale.