Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 13 décembre 2016
N° CERTFR-2016-AVI-407

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans le noyau Linux de Suse

Gestion du document

Référence	CERTFR-2016-AVI-407
Titre	Multiples vulnérabilités dans le noyau Linux de Suse
Date de la première version	13 décembre 2016
Date de la dernière version	23 décembre 2016
Source(s)	Bulletin de sécurité Suse SUSE-SU-2016:3094-1 du 12 décembre 2016 Bulletin de sécurité Suse SUSE-SU-2016:3100-1 du 12 décembre 2016 Bulletin de sécurité Suse SUSE-SU-2016:3093-1 du 12 décembre 2016 Bulletin de sécurité Suse SUSE-SU-2016:3098-1 du 12 décembre 2016 Bulletin de sécurité Suse SUSE-SU-2016:3104-1 du 12 décembre 2016 Bulletin de sécurité Suse SUSE-SU-2016:3096-1 du 12 décembre 2016 Bulletin de sécurité Suse SUSE-SU-2016:3111-1 du 13 décembre 2016 Bulletin de sécurité Suse SUSE-SU-2016:3112-1 du 13 décembre 2016 Bulletin de sécurité Suse SUSE-SU-2016:3113-1 du 13 décembre 2016 Bulletin de sécurité Suse SUSE-SU-2016:3109-1 du 13 décembre 2016 Bulletin de sécurité Suse SUSE-SU-2016:3117-1 du 13 décembre 2016 Bulletin de sécurité Suse SUSE-SU-2016:3116-1 du 13 décembre 2016 Bulletin de sécurité Suse SUSE-SU-2016:3169-1 du 15 décembre 2016 Bulletin de sécurité Suse SUSE-SU-2016:3183-1 du 16 décembre 2016 Bulletin de sécurité Suse SUSE-SU-2016:3197-1 du 20 décembre 2016 Bulletin de sécurité Suse SUSE-SU-2016:3205-1 du 21 décembre 2016 Bulletin de sécurité Suse SUSE-SU-2016:3206-1 du 21 décembre 2016 Bulletin de sécurité Suse SUSE-SU-2016:3249-1 du 22 décembre 2016
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 à distance
- déni de service à distance
- déni de service
- élévation de privilèges

2 - Systèmes affectés

- SUSE Linux Enterprise Live Patching 12
- SUSE Linux Enterprise Server 12-LTSS
- SUSE Linux Enterprise pour SAP 12

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 à distance, un déni de service à distance et un déni de service.

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-2016:3094-1 du 12 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163094-1.html
- Bulletin de sécurité Suse SUSE-SU-2016:3100-1 du 12 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163100-1.html
- Bulletin de sécurité Suse SUSE-SU-2016:3093-1 du 12 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163093-1.html
- Bulletin de sécurité Suse SUSE-SU-2016:3098-1 du 12 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163098-1.html
- Bulletin de sécurité Suse SUSE-SU-2016:3104-1 du 12 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163104-1.html
- Bulletin de sécurité Suse SUSE-SU-2016:3096-1 du 12 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163096-1.html
- Bulletin de sécurité Suse SUSE-SU-2016:3111-1 du 13 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163111-1.html
- Bulletin de sécurité Suse SUSE-SU-2016:3112-1 du 13 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163112-1.html
- Bulletin de sécurité Suse SUSE-SU-2016:3113-1 du 13 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163113-1.html
- Bulletin de sécurité Suse SUSE-SU-2016:3109-1 du 13 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163109-1.html
- Bulletin de sécurité Suse SUSE-SU-2016:3117-1 du 13 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163117-1.html
- Bulletin de sécurité Suse SUSE-SU-2016:3116-1 du 13 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163116-1.html
- Bulletin de sécurité Suse SUSE-SU-2016:3119-1 du 13 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163119-1.html
- Bulletin de sécurité Suse SUSE-SU-2016:3169-1 du 15 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163169-1.html
- Bulletin de sécurité Suse SUSE-SU-2016:3183-1 du 16 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163183-1.html
- Bulletin de sécurité Suse SUSE-SU-2016:3197-1 du 20 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163197-1.html
- Bulletin de sécurité Suse SUSE-SU-2016:3205-1 du 21 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163205-1.html
- Bulletin de sécurité Suse SUSE-SU-2016:3206-1 du 21 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163206-1.html

- Bulletin de sécurité Suse SUSE-SU-2016:3249-1 du 22 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163249-1.html
- Bulletin de sécurité Suse SUSE-SU-2016:3247-1 du 22 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163247-1.html
- Référence CVE CVE-2016-8655
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8655
- Référence CVE CVE-2016-9555
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9555
- Référence CVE CVE-2016-7117
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7117

Gestion détaillée du document

13 décembre 2016 version initiale.

13 décembre 2016 ajout de nouveaux bulletins de sécurité et mise à jour des systèmes affectés.

14 décembre 2016 ajout de nouveaux bulletins de sécurité.

19 décembre 2016 ajout de nouveaux bulletins de sécurité.

21 décembre 2016 ajout de nouveaux bulletins de sécurité et mise à jour des systèmes affectés.

22 décembre 2016 ajout de nouveaux bulletins de sécurité.

23 décembre 2016 ajout de nouveaux bulletins de sécurité.