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 15 décembre 2016
N° CERTFR-2016-AVI-420

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-420
Titre	Multiples vulnérabilités dans le noyau Linux de SUSE
Date de la première version	15 décembre 2016
Date de la dernière version	23 décembre 2016
Source(s)	Bulletin de sécurité SUSE SUSE-SU-2016:3146-1 du 14 décembre 2016 Bulletin de sécurité SUSE SUSE-SU-2016:3188-1 du 16 décembre 2016 Bulletin de sécurité SUSE SUSE-SU-2016:3203-1 du 20 décembre 2016 Bulletin de sécurité SUSE SUSE-SU-2016:3217-1 du 21 décembre 2016 Bulletin de sécurité SUSE SUSE-SU-2016:3248-1 du 22 décembre 2016 Bulletin de sécurité SUSE SUSE-SU-2016:3252-1 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)

- déni de service
- atteinte à l'intégrité des données
- élévation de privilèges

2 - Systèmes affectés

- SUSE Linux Enterprise Workstation Extension 12-SP1 12-SP2
- SUSE Linux Enterprise Software Development Kit 12-SP1, 12-SP2 11-SP4
- SUSE Linux Enterprise Server pour Raspberry Pi 12-SP2
- SUSE Linux Enterprise Server 12-SP1, 12-SP2, 11-SP4, 11-SP2-LTSS, 11-SP3-LTSS 11-EXTRA
- SUSE Linux Enterprise Server pour SAP 12
- SUSE Linux Enterprise Live Patching 12
- SUSE Linux Enterprise High Availability 12-SP2
- SUSE Linux Enterprise Desktop 12-SP1 12-SP2
- SUSE Linux Enterprise Module pour Public Cloud 12
- SUSE Linux Enterprise Debuginfo 11-SP2, 11-SP3, 11-SP4

- SUSE Linux Enterprise Point of Sale 11-SP3
- SUSE Linux Manager 2.1
- SUSE Linux Manager Proxy 2.1
- SUSE OpenStack Cloud 5

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *le noyau Linux de SUSE*. Elles permettent à un attaquant de provoquer un déni de service, une atteinte à l'intégrité des données et une élévation de privilèges.

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-2016:3146-1 du 14 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163146-1.html
- Bulletin de sécurité SUSE SUSE-SU-2016:3188-1 du 16 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163188-1.html
- Bulletin de sécurité SUSE SUSE-SU-2016:3203-1 du 20 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163203-1.html
- Bulletin de sécurité SUSE SUSE-SU-2016:3217-1 du 21 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163217-1.html
- Bulletin de sécurité SUSE SUSE-SU-2016:3248-1 du 22 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163248-1.html
- Bulletin de sécurité SUSE SUSE-SU-2016:3252-1 du 22 décembre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20163252-1.html
- Référence CVE CVE-2016-9576
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9576
- Référence CVE CVE-2016-9794
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9794

Gestion détaillée du document

15 décembre 2016 version initiale.
19 décembre 2016 ajout de nouveaux bulletins de sécurité et mise à jour des systèmes affectés.
20 décembre 2016 ajout de nouveaux bulletins de sécurité et mise à jour des systèmes affectés.
22 décembre 2016 ajout de nouveaux bulletins de sécurité et mise à jour des systèmes affectés.
23 décembre 2016 ajout de nouveaux bulletins de sécurité et mise à jour des systèmes affectés.