

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans le noyau Linux de Suse

Gestion du document

Référence	CERTFR-2017-AVI-026
Titre	Multiples vulnérabilités dans le noyau Linux de Suse
Date de la première version	23 janvier 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité Suse suse-su-20170227-1 du 21 janvier 2017 Bulletin de sécurité Suse suse-su-20170228-1 du 21 janvier 2017 Bulletin de sécurité Suse suse-su-20170231-1 du 21 janvier 2017 Bulletin de sécurité Suse suse-su-20170232-1 du 21 janvier 2017 Bulletin de sécurité Suse suse-su-20170233-1 du 21 janvier 2017 Bulletin de sécurité Suse suse-su-20170234-1 du 21 janvier 2017 Bulletin de sécurité Suse suse-su-20170235-1 du 21 janvier 2017 Bulletin de sécurité Suse suse-su-20170230-1 du 21 janvier 2017 Bulletin de sécurité Suse suse-su-20170226-1 du 21 janvier 2017 Bulletin de sécurité Suse suse-su-20170229-1 du 21 janvier 2017 Bulletin de sécurité Suse suse-su-20170247-1 du 21 janvier 2017 Bulletin de sécurité Suse suse-su-20170244-1 du 21 janvier 2017 Bulletin de sécurité Suse suse-su-20170249-1 du 21 janvier 2017 Bulletin de sécurité Suse suse-su-20170248-1 du 21 janvier 2017 Bulletin de sécurité Suse suse-su-20170246-1 du 21 janvier 2017 Bulletin de sécurité Suse suse-su-20170245-1 du 21 janvier 2017
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)

- non spécifié par l'éditeur
- déni de service
- atteinte à l'intégrité des données
- atteinte à la confidentialité des données
- élévation de privilèges

2 - Systèmes affectés

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

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *le noyau Linux de Suse*. Certaines d'entre elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur, un déni de service et une atteinte à l'intégrité 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-20170227-1 du 21 janvier 2017
<https://www.suse.com/support/update/announcement/2017/suse-su-20170227-1.html>
- Bulletin de sécurité Suse suse-su-20170228-1 du 21 janvier 2017
<https://www.suse.com/support/update/announcement/2017/suse-su-20170228-1.html>
- Bulletin de sécurité Suse suse-su-20170231-1 du 21 janvier 2017
<https://www.suse.com/support/update/announcement/2017/suse-su-20170231-1.html>
- Bulletin de sécurité Suse suse-su-20170232-1 du 21 janvier 2017
<https://www.suse.com/support/update/announcement/2017/suse-su-20170232-1.html>
- Bulletin de sécurité Suse suse-su-20170233-1 du 21 janvier 2017
<https://www.suse.com/support/update/announcement/2017/suse-su-20170233-1.html>
- Bulletin de sécurité Suse suse-su-20170234-1 du 21 janvier 2017
<https://www.suse.com/support/update/announcement/2017/suse-su-20170234-1.html>
- Bulletin de sécurité Suse suse-su-20170235-1 du 21 janvier 2017
<https://www.suse.com/support/update/announcement/2017/suse-su-20170235-1.html>
- Bulletin de sécurité Suse suse-su-20170230-1 du 21 janvier 2017
<https://www.suse.com/support/update/announcement/2017/suse-su-20170230-1.html>
- Bulletin de sécurité Suse suse-su-20170226-1 du 21 janvier 2017
<https://www.suse.com/support/update/announcement/2017/suse-su-20170226-1.html>
- Bulletin de sécurité Suse suse-su-20170229-1 du 21 janvier 2017
<https://www.suse.com/support/update/announcement/2017/suse-su-20170229-1.html>
- Bulletin de sécurité Suse suse-su-20170247-1 du 21 janvier 2017
<https://www.suse.com/support/update/announcement/2017/suse-su-20170247-1.html>
- Bulletin de sécurité Suse suse-su-20170244-1 du 21 janvier 2017
<https://www.suse.com/support/update/announcement/2017/suse-su-20170244-1.html>
- Bulletin de sécurité Suse suse-su-20170249-1 du 21 janvier 2017
<https://www.suse.com/support/update/announcement/2017/suse-su-20170249-1.html>
- Bulletin de sécurité Suse suse-su-20170248-1 du 21 janvier 2017
<https://www.suse.com/support/update/announcement/2017/suse-su-20170248-1.html>
- Bulletin de sécurité Suse suse-su-20170246-1 du 21 janvier 2017
<https://www.suse.com/support/update/announcement/2017/suse-su-20170246-1.html>
- Bulletin de sécurité Suse suse-su-20170245-1 du 21 janvier 2017
<https://www.suse.com/support/update/announcement/2017/suse-su-20170245-1.html>
- Référence CVE CVE-2016-10088
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10088>
- Référence CVE CVE-2016-8632
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8632>

- 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>
- Référence CVE CVE-2016-9806
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9806>

Gestion détaillée du document

23 janvier 2017 version initiale.

Conditions d'utilisation de ce document : <http://cert.ssi.gouv.fr/cert-fr/apropos.html>
Dernière version de ce document : <http://cert.ssi.gouv.fr/site/CERTFR-2017-AVI-026>
