

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-131
Titre	Multiples vulnérabilités dans le noyau Linux de Suse
Date de la première version	15 avril 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Suse suse-su-20161031-1 du 14 avril 2016 Bulletin de sécurité Suse suse-su-20161032-1 du 14 avril 2016 Bulletin de sécurité Suse suse-su-20161035-1 du 14 avril 2016 Bulletin de sécurité Suse suse-su-20161033-1 du 14 avril 2016 Bulletin de sécurité Suse suse-su-20161040-1 du 14 avril 2016 Bulletin de sécurité Suse suse-su-20161038-1 du 14 avril 2016 Bulletin de sécurité Suse suse-su-20161037-1 du 14 avril 2016 Bulletin de sécurité Suse suse-su-20161041-1 du 14 avril 2016 Bulletin de sécurité Suse suse-su-20161039-1 du 14 avril 2016 Bulletin de sécurité Suse suse-su-20161034-1 du 14 avril 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
- élévation de privilèges

2 - Systèmes affectés

SUSE Linux Enterprise Live Patching 12

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 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-20161031-1 du 14 avril 2016
<https://www.suse.com/support/update/announcement/2016/suse-su-20161031-1.html>
- Bulletin de sécurité Suse suse-su-20161032-1 du 14 avril 2016
<https://www.suse.com/support/update/announcement/2016/suse-su-20161032-1.html>
- Bulletin de sécurité Suse suse-su-20161035-1 du 14 avril 2016
<https://www.suse.com/support/update/announcement/2016/suse-su-20161035-1.html>
- Bulletin de sécurité Suse suse-su-20161033-1 du 14 avril 2016
<https://www.suse.com/support/update/announcement/2016/suse-su-20161033-1.html>
- Bulletin de sécurité Suse suse-su-20161040-1 du 14 avril 2016
<https://www.suse.com/support/update/announcement/2016/suse-su-20161040-1.html>
- Bulletin de sécurité Suse suse-su-20161038-1 du 14 avril 2016
<https://www.suse.com/support/update/announcement/2016/suse-su-20161038-1.html>
- Bulletin de sécurité Suse suse-su-20161037-1 du 14 avril 2016
<https://www.suse.com/support/update/announcement/2016/suse-su-20161037-1.html>
- Bulletin de sécurité Suse suse-su-20161041-1 du 14 avril 2016
<https://www.suse.com/support/update/announcement/2016/suse-su-20161041-1.html>
- Bulletin de sécurité Suse suse-su-20161039-1 du 14 avril 2016
<https://www.suse.com/support/update/announcement/2016/suse-su-20161039-1.html>
- Bulletin de sécurité Suse suse-su-20161034-1 du 14 avril 2016
<https://www.suse.com/support/update/announcement/2016/suse-su-20161034-1.html>
- Référence CVE CVE-2015-8709
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8709>
- Référence CVE CVE-2015-8812
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8812>
- Référence CVE CVE-2016-0774
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0774>
- Référence CVE CVE-2016-2384
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2384>

Gestion détaillée du document

15 avril 2016 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-2016-AVI-131>
