

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-141
Titre	Multiples vulnérabilités dans le noyau Linux de SUSE
Date de la première version	09 mai 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité SUSE suse-su-20171183-1 du 05 mai 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 à distance
- déni de service
- élévation de privilèges

2 - Systèmes affectés

- SUSE Linux Enterprise Workstation Extension 12-SP2
- SUSE Linux Enterprise Software Development Kit 12-SP2
- SUSE Linux Enterprise Server for Raspberry Pi 12-SP2
- SUSE Linux Enterprise Server 12-SP2
- SUSE Linux Enterprise Live Patching 12
- SUSE Linux Enterprise High Availability 12-SP2
- SUSE Linux Enterprise Desktop 12-SP2
- OpenStack Cloud Magnum Orchestration 7

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 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-20171183-1 du 05 mai 2017
<https://www.suse.com/support/update/announcement/2017/suse-su-20171183-1/>
- Référence CVE CVE-2016-1020
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1020>
- Référence CVE CVE-2016-2117
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2117>
- Référence CVE CVE-2016-9191
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9191>
- Référence CVE CVE-2017-2596
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2596>
- Référence CVE CVE-2017-2671
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2671>
- Référence CVE CVE-2017-5986
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5986>
- Référence CVE CVE-2017-6074
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6074>
- Référence CVE CVE-2017-6214
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6214>
- Référence CVE CVE-2017-6345
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6345>
- Référence CVE CVE-2017-6346
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6346>
- Référence CVE CVE-2017-6347
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6347>
- Référence CVE CVE-2017-6353
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6353>
- Référence CVE CVE-2017-7187
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7187>
- Référence CVE CVE-2017-7261
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7261>
- Référence CVE CVE-2017-7294
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7294>
- Référence CVE CVE-2017-7308
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7308>
- Référence CVE CVE-2017-7374
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7374>

Gestion détaillée du document

09 mai 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-141>
