

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans le noyau Linux SUSE

Gestion du document

Référence	CERTFR-2017-AVI-050
Titre	Multiples vulnérabilités dans le noyau Linux SUSE
Date de la première version	15 février 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité SUSE SUSE-SU-2017:0464-1 du 14 février 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)

- exécution de code arbitraire à distance
- exécution de code arbitraire
- déni de service
- atteinte à l'intégrité des données
- atteinte à la confidentialité des données
- élévation de privilèges

2 - Systèmes affectés

- SUSE Linux Enterprise Workstation Extension 12-SP1
- SUSE Linux Enterprise Software Development Kit 12-SP1
- SUSE Linux Enterprise Server 12-SP1
- SUSE Linux Enterprise Module for Public Cloud 12
- SUSE Linux Enterprise Live Patching 12
- SUSE Linux Enterprise Desktop 12-SP1

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, une exécution de code arbitraire 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-2017:0464-1 du 14 février 2017
<https://www.suse.com/support/update/announcement/2017/suse-su-20170464-1.html>
- Référence CVE CVE-2015-8962
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8962>
- Référence CVE CVE-2015-8963
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8963>
- Référence CVE CVE-2015-8964
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8964>
- Référence CVE CVE-2016-1008
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1008>
- Référence CVE CVE-2016-7910
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7910>
- Référence CVE CVE-2016-7911
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7911>
- Référence CVE CVE-2016-7913
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7913>
- Référence CVE CVE-2016-7914
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7914>
- Référence CVE CVE-2016-8399
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8399>
- Référence CVE CVE-2016-8633
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8633>
- Référence CVE CVE-2016-8645
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8645>
- Référence CVE CVE-2016-9083
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9083>
- Référence CVE CVE-2016-9084
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9084>
- Référence CVE CVE-2016-9756
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9756>
- Référence CVE CVE-2016-9793
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9793>
- Référence CVE CVE-2016-9806
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9806>
- Référence CVE CVE-2017-2583
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2583>
- Référence CVE CVE-2017-2584
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2584>
- Référence CVE CVE-2017-5551
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5551>

Gestion détaillée du document

15 février 2017 version initiale.