

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-131
Titre	Multiples vulnérabilités dans le noyau Linux de SUSE
Date de la première version	26 avril 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité SUSE SUSE-SU-2017:1102-1 du 25 avril 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
- déni de service à distance
- déni de service
- atteinte à l'intégrité des données
- atteinte à la confidentialité des données
- élévation de privilèges

2 - Systèmes affectés

- SUSE Linux Enterprise Real Time Extension 11-SP4
- SUSE Linux Enterprise Debuginfo 11-SP4

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, 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-2017:1102-1 du 25 avril 2017
<https://www.suse.com/support/update/announcement/2017/suse-su-20171102-1/>
- Référence CVE CVE-2004-0230
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-0230>
- Référence CVE CVE-2012-6704
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-6704>
- Référence CVE CVE-2013-6368
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6368>
- Référence CVE CVE-2015-1350
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1350>
- Référence CVE CVE-2015-8956
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8956>
- Référence CVE CVE-2015-8962
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8962>
- 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-2016-3841
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3841>
- Référence CVE CVE-2016-5696
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5696>
- Référence CVE CVE-2016-7042
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7042>
- Référence CVE CVE-2016-7097
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7097>
- Référence CVE CVE-2016-7117
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7117>
- 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-2016-7916
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7916>
- Référence CVE CVE-2016-8399
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8399>
- Référence CVE CVE-2016-8632
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8632>
- Référence CVE CVE-2016-8633
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8633>
- Référence CVE CVE-2016-8646
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8646>
- Référence CVE CVE-2016-9555
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9555>
- Référence CVE CVE-2016-9576
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9576>
- Référence CVE CVE-2016-9685
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9685>

- 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-2016-9794
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9794>
- Référence CVE CVE-2017-5551
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5551>

Gestion détaillée du document

26 avril 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-131>
