Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 16 mai 2017
N° CERTFR-2017-AVI-156

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-156
Titre	Multiples vulnérabilités dans le noyau Linux de Suse
Date de la première version	16 mai 2017
Date de la dernière version	17 mai 2017
Source(s)	Bulletin de sécurité Suse suse-su-20171301-1 du 15 mai 2017 Bulletin de sécurité Suse suse-su-20171281-1 du 15 mai 2017 Bulletin de sécurité Suse suse-su-20171302-1 du 15 mai 2017 Bulletin de sécurité Suse suse-su-20171287-1 du 15 mai 2017 Bulletin de sécurité Suse suse-su-20171278-1 du 15 mai 2017 Bulletin de sécurité Suse suse-su-20171291-1 du 15 mai 2017 Bulletin de sécurité Suse suse-su-20171300-1 du 15 mai 2017 Bulletin de sécurité Suse suse-su-20171283-1 du 15 mai 2017 Bulletin de sécurité Suse suse-su-20171295-1 du 15 mai 2017 Bulletin de sécurité Suse suse-su-20171277-1 du 15 mai 2017 Bulletin de sécurité Suse suse-su-20171279-1 du 15 mai 2017 Bulletin de sécurité Suse suse-su-20171280-1 du 15 mai 2017 Bulletin de sécurité Suse suse-su-20171294-1 du 15 mai 2017 Bulletin de sécurité Suse suse-su-20171290-1 du 15 mai 2017 Bulletin de sécurité Suse suse-su-20171289-1 du 15 mai 2017 Bulletin de sécurité Suse suse-su-20171297-1 du 15 mai 2017 Bulletin de sécurité Suse suse-su-20171288-1 du 15 mai 2017 Bulletin de sécurité Suse suse-su-20171284-1 du 15 mai 2017 Bulletin de sécurité Suse suse-su-20171293-1 du 15 mai 2017 Bulletin de sécurité Suse suse-su-20171285-1 du 15 mai 2017 Bulletin de sécurité Suse suse-su-20171299-1 du 15 mai 2017 Bulletin de sécurité Suse suse-su-20171303-1 du 15 mai 2017 Bulletin de sécurité Suse suse-su-20171308-1 du 16 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
- contournement de la politique de sécurité
- atteinte à l'intégrité des données
- atteinte à la confidentialité des données
- élévation de privilèges

2 - Systèmes affectés

- SUSE Linux Enterprise Software Development Kit 11-SP4
- SUSE Linux Enterprise Server 11-SP4
- SUSE Linux Enterprise Server 11-EXTRA
- SUSE Linux Enterprise Debuginfo 11-SP4
- SUSE Linux Enterprise Server for SAP 12
- SUSE Linux Enterprise Server 12-LTSS
- SUSE Linux Enterprise Live Patching 12

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-20171301-1 du 15 mai 2017
  https://www.suse.com/support/update/announcement/2017/suse-su-20171301-1/
- Bulletin de sécurité Suse suse-su-20171281-1 du 15 mai 2017
  https://www.suse.com/support/update/announcement/2017/suse-su-20171281-1/
- Bulletin de sécurité Suse suse-su-20171302-1 du 15 mai 2017
  https://www.suse.com/support/update/announcement/2017/suse-su-20171302-1/
- Bulletin de sécurité Suse suse-su-20171287-1 du 15 mai 2017
  https://www.suse.com/support/update/announcement/2017/suse-su-20171287-1/
- Bulletin de sécurité Suse suse-su-20171278-1 du 15 mai 2017
  https://www.suse.com/support/update/announcement/2017/suse-su-20171278-1/
- Bulletin de sécurité Suse suse-su-20171291-1 du 15 mai 2017
  https://www.suse.com/support/update/announcement/2017/suse-su-20171291-1/
- Bulletin de sécurité Suse suse-su-20171300-1 du 15 mai 2017
  https://www.suse.com/support/update/announcement/2017/suse-su-20171300-1/
- Bulletin de sécurité Suse suse-su-20171283-1 du 15 mai 2017
  https://www.suse.com/support/update/announcement/2017/suse-su-20171283-1/
- Bulletin de sécurité Suse suse-su-20171295-1 du 15 mai 2017
  https://www.suse.com/support/update/announcement/2017/suse-su-20171295-1/
- Bulletin de sécurité Suse suse-su-20171277-1 du 15 mai 2017
  https://www.suse.com/support/update/announcement/2017/suse-su-20171277-1/

- Bulletin de sécurité Suse suse-su-20171279-1 du 15 mai 2017
  https://www.suse.com/support/update/announcement/2017/suse-su-20171279-1/
- Bulletin de sécurité Suse suse-su-20171280-1 du 15 mai 2017
  https://www.suse.com/support/update/announcement/2017/suse-su-20171280-1/
- Bulletin de sécurité Suse suse-su-20171294-1 du 15 mai 2017
  https://www.suse.com/support/update/announcement/2017/suse-su-20171294-1/
- Bulletin de sécurité Suse suse-su-20171290-1 du 15 mai 2017
  https://www.suse.com/support/update/announcement/2017/suse-su-20171290-1/
- Bulletin de sécurité Suse suse-su-20171289-1 du 15 mai 2017
  https://www.suse.com/support/update/announcement/2017/suse-su-20171289-1/
- Bulletin de sécurité Suse suse-su-20171297-1 du 15 mai 2017
  https://www.suse.com/support/update/announcement/2017/suse-su-20171297-1/
- Bulletin de sécurité Suse suse-su-20171288-1 du 15 mai 2017
  https://www.suse.com/support/update/announcement/2017/suse-su-20171288-1/
- Bulletin de sécurité Suse suse-su-20171284-1 du 15 mai 2017
  https://www.suse.com/support/update/announcement/2017/suse-su-20171284-1/
- Bulletin de sécurité Suse suse-su-20171293-1 du 15 mai 2017
  https://www.suse.com/support/update/announcement/2017/suse-su-20171293-1/
- Bulletin de sécurité Suse suse-su-20171285-1 du 15 mai 2017
  https://www.suse.com/support/update/announcement/2017/suse-su-20171285-1/
- Bulletin de sécurité Suse suse-su-20171299-1 du 15 mai 2017
  https://www.suse.com/support/update/announcement/2017/suse-su-20171299-1/
- Bulletin de sécurité Suse suse-su-20171303-1 du 15 mai 2017
  https://www.suse.com/support/update/announcement/2017/suse-su-20171303-1/
- Bulletin de sécurité Suse suse-su-20171303-1 du 16 mai 2017
  https://www.suse.com/support/update/announcement/2017/suse-su-20171308-1/
- Référence CVE CVE-2015-3288
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3288
- Référence CVE CVE-2015-8970
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8970
- Référence CVE CVE-2016-1020
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1020
- Référence CVE CVE-2016-5243
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5243
- Référence CVE CVE-2017-2671
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2671
- Référence CVE CVE-2017-5669
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5669
- Référence CVE CVE-2017-5970
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5970
- 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-2017-6348
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6348
- Référence CVE CVE-2017-6353
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6353
- Référence CVE CVE-2017-7184
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7184
- 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-2017-7616
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7616

Gestion détaillée du document

16 mai 2017 version initiale.

17 mai 2017 ajout du bulletin de sécurité Suse suse-su-20171308-1.