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 26 octobre 2016
N° CERTFR-2016-AVI-362

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-362
Titre	Multiples vulnérabilités dans le noyau Linux de Suse
Date de la première version	26 octobre 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Suse suse-su-20162633-1 du 25 octobre 2016 Bulletin de sécurité Suse suse-su-20162635-1 du 25 octobre 2016 Bulletin de sécurité Suse suse-su-20162634-1 du 25 octobre 2016 Bulletin de sécurité Suse suse-su-20162638-1 du 25 octobre 2016 Bulletin de sécurité Suse suse-su-20162637-1 du 25 octobre 2016 Bulletin de sécurité Suse suse-su-20162636-1 du 25 octobre 2016 Bulletin de sécurité Suse suse-su-20162632-1 du 25 octobre 2016 Bulletin de sécurité Suse suse-su-20162631-1 du 25 octobre 2016 Bulletin de sécurité Suse suse-su-20162629-1 du 25 octobre 2016 Bulletin de sécurité Suse suse-su-20162630-1 du 25 octobre 2016 Bulletin de sécurité Suse suse-su-20162614-1 du 24 octobre 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 à distance
- élévation de privilèges

2 - Systèmes affectés

- SUSE Linux Enterprise Server for SAP 12
- SUSE Linux Enterprise Server 12-LTSS
- SUSE Linux Enterprise Live Patching 12
- SUSE OpenStack Cloud 5
- SUSE Manager Proxy 2.1
- SUSE Manager 2.1

- SUSE Linux Enterprise Server 11-EXTRA
- SUSE Linux Enterprise Point of Sale 11-SP3
- SUSE Linux Enterprise Debuginfo 11-SP3

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 à distance 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-20162633-1 du 25 octobre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20162633-1.html
- Bulletin de sécurité Suse suse-su-20162635-1 du 25 octobre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20162635-1.html
- Bulletin de sécurité Suse suse-su-20162634-1 du 25 octobre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20162634-1.html
- Bulletin de sécurité Suse suse-su-20162638-1 du 25 octobre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20162638-1.html
- Bulletin de sécurité Suse suse-su-20162637-1 du 25 octobre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20162637-1.html
- Bulletin de sécurité Suse suse-su-20162636-1 du 25 octobre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20162636-1.html
- Bulletin de sécurité Suse suse-su-20162632-1 du 25 octobre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20162632-1.html
- Bulletin de sécurité Suse suse-su-20162631-1 du 25 octobre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20162631-1.html
- Bulletin de sécurité Suse suse-su-20162629-1 du 25 octobre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20162629-1.html
- Bulletin de sécurité Suse suse-su-20162630-1 du 25 octobre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20162630-1.html
- Bulletin de sécurité Suse suse-su-20162614-1 du 24 octobre 2016
  https://www.suse.com//support/update/announcement/2016/suse-su-20162614-1.html
- Référence CVE CVE-2016-5195
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5195
- Référence CVE CVE-2016-8666
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8666
- Référence CVE CVE-2016-4997
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4997

Gestion détaillée du document

26 octobre 2016 version initiale.