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 07 juin 2017
N° CERTFR-2017-AVI-169

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans le noyau Linux d'Ubuntu

Gestion du document

Référence	CERTFR-2017-AVI-169
Titre	Multiples vulnérabilités dans le noyau Linux d'Ubuntu
Date de la première version	07 juin 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité Ubuntu USN-3312-1 du 06 juin 2017 Bulletin de sécurité Ubuntu USN-3312-2 du 06 juin 2017 Bulletin de sécurité Ubuntu USN-3313-1 du 06 juin 2017 Bulletin de sécurité Ubuntu USN-3313-2 du 07 juin 2017 Bulletin de sécurité Ubuntu USN-3314-1 du 07 juin 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 à distance
- déni de service
- contournement de la politique de sécurité
- atteinte à la confidentialité des données
- élévation de privilèges

2 - Systèmes affectés

- Ubuntu 14.04 LTS
- Ubuntu 16.04 LTS
- Ubuntu 16.10
- Ubuntu 17.04

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *le noyau Linux d'Ubuntu*. 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 à distance.

4 - Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 - Documentation

- Bulletin de sécurité Ubuntu USN-3312-1 du 06 juin 2017
  https://www.ubuntu.com/usn/usn-3312-1/
- Bulletin de sécurité Ubuntu usn-3312-2 du 06 juin 2017
  https://www.ubuntu.com/usn/usn-3312-2/
- Bulletin de sécurité Ubuntu USN-3312-2 du 06 juin 2017
  https://www.ubuntu.com/usn/usn-3312-2/
- Bulletin de sécurité Ubuntu USN-3313-1 du 06 juin 2017
  https://www.ubuntu.com/usn/usn-3313-1/
- Bulletin de sécurité Ubuntu USN-3313-2 du 07 juin 2017
  https://www.ubuntu.com/usn/usn-3313-2/
- Bulletin de sécurité Ubuntu USN-3314-1 du 07 juin 2017
  https://www.ubuntu.com/usn/usn-3314-1/
- Référence CVE CVE-2016-7913
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7913
- Référence CVE CVE-2016-7917
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7917
- Référence CVE CVE-2016-8632
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8632
- 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-2016-9604
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9604
- Référence CVE CVE-2017-0605
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0605
- 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-2017-6001
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6001
- Référence CVE CVE-2017-7277
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7277
- Référence CVE CVE-2017-7472
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7472
- Référence CVE CVE-2017-7618
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7618
- Référence CVE CVE-2017-7645
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7645

- Référence CVE CVE-2017-7889
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7889
- Référence CVE CVE-2017-7895
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7895
- Référence CVE CVE-2017-7979
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7979
- Référence CVE CVE-2017-8063
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8063
- Référence CVE CVE-2017-8064
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8064
- Référence CVE CVE-2017-8067
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8067

Gestion détaillée du document

07 juin 2017 version initiale.