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 août 2017
N° CERTFR-2017-AVI-267

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans le noyau Linux de RedHat

Gestion du document

Référence	CERTFR-2017-AVI-267
Titre	Multiples vulnérabilités dans le noyau Linux de RedHat
Date de la première version	16 août 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité RedHat RHSA-2017:2473 du 15 août 2017 Bulletin de sécurité RedHat RHSA-2017:2472 du 15 août 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

2 - Systèmes affectés

- Red Hat Enterprise Linux Server - AUS 5.9 x86_64, ia64 et i386
- Red Hat Enterprise Linux Server 7 x86_64
- Red Hat Enterprise Linux Server - Extended Update Support 7.4 x86_64
- Red Hat Enterprise Linux Server - AUS 7.4 x86_64
- Red Hat Enterprise Linux Workstation 7 x86_64
- Red Hat Enterprise Linux Desktop 7 x86_64
- Red Hat Enterprise Linux pour IBM z Systems 7 s390x
- Red Hat Enterprise Linux pour IBM z Systems - Extended Update Support 7.4 s390x
- Red Hat Enterprise Linux pour Power, big endian 7 ppc64
- Red Hat Enterprise Linux pour Power, big endian - Extended Update Support 7.4 ppc64
- Red Hat Enterprise Linux pour Scientific Computing 7 x86_64
- Red Hat Enterprise Linux EUS Compute Node 7.4 x86_64
- Red Hat Enterprise Linux pour Power, little endian 7 ppc64le

- Red Hat Enterprise Linux pour Power, little endian - Extended Update Support 7.4 ppc64le
- Red Hat Enterprise Linux Server pour ARM 7 aarch64
- Red Hat Virtualization Host 4 x86_64
- Red Hat Enterprise Linux Server - TUS 7.4 x86_64

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *le noyau Linux de RedHat*. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une atteinte à l'intégrité des données.

4 - Solution

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

5 - Documentation

- Bulletin de sécurité RedHat RHSA-2017:2473 du 15 août 2017
  https://access.redhat.com/errata/RHSA-2017:2473
- Bulletin de sécurité RedHat RHSA-2017:2472 du 15 août 2017
  https://access.redhat.com/errata/RHSA-2017:2472
- Référence CVE CVE-2017-7533
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7533
- Référence CVE CVE-2017-7895
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7895

Gestion détaillée du document

16 août 2017 version initiale.