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 09 août 2017
N° CERTFR-2017-AVI-262

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-262
Titre	Multiples vulnérabilités dans le noyau Linux de RedHat
Date de la première version	09 août 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité RedHat RHSA-2017:2428 du 08 août 2017 Bulletin de sécurité RedHat RHSA-2017:2429 du 08 août 2017 Bulletin de sécurité RedHat RHSA-2017:2437 du 08 août 2017 Bulletin de sécurité RedHat RHSA-2017:2444 du 08 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)

- non spécifié par l'éditeur
- déni de service
- élévation de privilèges

2 - Systèmes affectés

- Red Hat Enterprise Linux Server - AUS 6.5 x86_64
- Red Hat Enterprise Linux Server - TUS 6.5 x86_64
- Red Hat Enterprise Linux Server - Extended Update Support 6.7 x86_64
- Red Hat Enterprise Linux Server - Extended Update Support 6.7 i386
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 6.7 s390x
- Red Hat Enterprise Linux for Power, big endian - Extended Update Support 6.7 ppc64
- Red Hat Enterprise Linux EUS Compute Node 6.7 x86_64
- Red Hat Enterprise Linux Server - Extended Update Support 7.3 x86_64
- Red Hat Enterprise Linux Server - AUS 7.3 x86_64
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 7.3 s390x

- Red Hat Enterprise Linux for Power, big endian - Extended Update Support 7.3 ppc64
- Red Hat Enterprise Linux EUS Compute Node 7.3 x86_64
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 7.3 ppc64le
- Red Hat Enterprise Linux Server - TUS 7.3 x86_64
- MRG Realtime 2 x86_64

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *le noyau Linux de RedHat*. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur, un déni de service 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 RedHat RHSA-2017:2428 du 08 août 2017
  https://access.redhat.com/errata/RHSA-2017:2428
- Bulletin de sécurité RedHat RHSA-2017:2429 du 08 août 2017
  https://access.redhat.com/errata/RHSA-2017:2429
- Bulletin de sécurité RedHat RHSA-2017:2437 du 08 août 2017
  https://access.redhat.com/errata/RHSA-2017:2437
- Bulletin de sécurité RedHat RHSA-2017:2444 du 08 août 2017
  https://access.redhat.com/errata/RHSA-2017:2444
- Référence CVE CVE-2015-8970
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8970
- Référence CVE CVE-2016-10200
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10200
- Référence CVE CVE-2017-2647
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2647
- Référence CVE CVE-2017-7895
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7895
- Référence CVE CVE-2017-8797
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8797

Gestion détaillée du document

09 août 2017 version initiale.