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 13 septembre 2017
N° CERTFR-2017-AVI-291

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans le noyau Linux de Red Hat

Gestion du document

Référence	CERTFR-2017-AVI-291
Titre	Multiples vulnérabilités dans le noyau Linux de Red Hat
Date de la première version	13 septembre 2017
Date de la dernière version	14 septembre 2017
Source(s)	Bulletin de sécurité Red Hat RHSA-2017:2679 du 12 septembre 2017 Bulletin de sécurité Red Hat RHSA-2017:2680 du 12 septembre 2017 Bulletin de sécurité Red Hat RHSA-2017:2681 du 12 septembre 2017 Bulletin de sécurité Red Hat RHSA-2017:2682 du 12 septembre 2017 Bulletin de sécurité Red Hat RHSA-2017:2683 du 12 septembre 2017 Bulletin de sécurité Red Hat RHSA-2017:2704 du 13 septembre 2017 Bulletin de sécurité Red Hat RHSA-2017:2705 du 13 septembre 2017 Bulletin de sécurité Red Hat RHSA-2017:2706 du 13 septembre 2017 Bulletin de sécurité Red Hat RHSA-2017:2707 du 13 septembre 2017 Bulletin de sécurité Red Hat RHSA-2017:2731 du 14 septembre 2017 Bulletin de sécurité Red Hat RHSA-2017:2732 du 14 septembre 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
- Non spécifié par l'éditeur

2 - Systèmes affectés

- MRG Realtime 2 x86_64
- Red Hat Enterprise Linux Desktop 6 i386 et x86_64
- Red Hat Enterprise Linux Desktop 7 x86_64
- Red Hat Enterprise Linux EUS Compute Node 6.7 x86_64

- Red Hat Enterprise Linux EUS Compute Node 7.2 x86_64
- Red Hat Enterprise Linux EUS Compute Node 7.3 x86_64
- Red Hat Enterprise Linux EUS Compute Node 7.4 x86_64
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 7.2 s390x
- Red Hat Enterprise Linux for Power, big endian - Extended Update Support 7.2 ppc64
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 7.2 ppc64le
- Red Hat Enterprise Linux High Availability - 4 Year Extended Update Support 7.2 x86_64
- Red Hat Enterprise Linux pour IBM z Systems 6 s390x
- Red Hat Enterprise Linux pour IBM z Systems 7 s390x
- Red Hat Enterprise Linux pour IBM z Systems - Extended Update Support 6.7 s390x
- Red Hat Enterprise Linux pour IBM z Systems - Extended Update Support 7.3 s390x
- Red Hat Enterprise Linux pour IBM z Systems - Extended Update Support 7.4 s390x
- Red Hat Enterprise Linux pour Power, big endian 6 ppc64
- Red Hat Enterprise Linux pour Power, big endian 7 ppc64 et Power, big endian - Extended Update Support 7.4 ppc64
- Red Hat Enterprise Linux pour Power, big endian - Extended Update Support 6.7 ppc64
- Red Hat Enterprise Linux pour Power, big endian - Extended Update Support 7.3 ppc64
- Red Hat Enterprise Linux pour Power, little endian 7 ppc64le et Power, little endian - Extended Update Support 7.4 ppc64le
- Red Hat Enterprise Linux pour Power, little endian - Extended Update Support 7.3 ppc64le
- Red Hat Enterprise Linux pour Real Time 7 x86_64
- Red Hat Enterprise Linux pour Real Time pour NFV 7 x86_64
- Red Hat Enterprise Linux pour Scientific Computing 6 x86_64
- Red Hat Enterprise Linux pour Scientific Computing 7 x86_64
- Red Hat Enterprise Linux Server - 4 Year Extended Update Support 7.2 x86_64
- Red Hat Enterprise Linux Server - 4 Year Extended Update Support 7.3 x86_64
- Red Hat Enterprise Linux Server - 4 Year Extended Update Support 7.4 x86_64
- Red Hat Enterprise Linux Server 6 i386 et x86_64
- Red Hat Enterprise Linux Server 7 x86_64
- Red Hat Enterprise Linux Server - AUS 6.2 x86_64
- Red Hat Enterprise Linux Server - AUS 6.4 x86_64
- Red Hat Enterprise Linux Server - AUS 6.5 x86_64
- Red Hat Enterprise Linux Server - AUS 6.6 x86_64
- Red Hat Enterprise Linux Server - AUS 7.2 x86_64
- Red Hat Enterprise Linux Server - AUS 7.3 x86_64
- Red Hat Enterprise Linux Server - AUS 7.4 x86_64
- Red Hat Enterprise Linux Server - Extended Update Support 6.7 i386 et x86_64
- Red Hat Enterprise Linux Server - Extended Update Support 7.2 x86_64
- Red Hat Enterprise Linux Server - Extended Update Support 7.3 x86_64
- Red Hat Enterprise Linux Server - Extended Update Support 7.4 x86_64
- Red Hat Enterprise Linux Server pour ARM 7 aarch64
- Red Hat Enterprise Linux Server (pour IBM Power LE) - 4 Year Extended Update Support 7.3 ppc64le
- Red Hat Enterprise Linux Server (pour IBM Power LE) - 4 Year Extended Update Support 7.4 ppc64le
- Red Hat Enterprise Linux Server - TUS 6.5 x86_64
- Red Hat Enterprise Linux Server - TUS 6.6 x86_64
- Red Hat Enterprise Linux Server - TUS 7.2 x86_64
- Red Hat Enterprise Linux Server - TUS 7.3 x86_64
- Red Hat Enterprise Linux Server - TUS 7.4 x86_64
- Red Hat Enterprise Linux Workstation 6 i386 et x86_64
- Red Hat Enterprise Linux Workstation 7 x86_64
- Red Hat Virtualization Host 4 x86_64
- RHEL for SAP - 4 Year Extended Update Support 7.2 x86_64

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *le noyau Linux de Red Hat*. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance 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 Red Hat RHSA-2017:2679 du 12 septembre 2017
  https://access.redhat.com/errata/RHSA-2017:2679
- Bulletin de sécurité Red Hat RHSA-2017:2680 du 12 septembre 2017
  https://access.redhat.com/errata/RHSA-2017:2680
- Bulletin de sécurité Red Hat RHSA-2017:2681 du 12 septembre 2017
  https://access.redhat.com/errata/RHSA-2017:2681
- Bulletin de sécurité Red Hat RHSA-2017:2682 du 12 septembre 2017
  https://access.redhat.com/errata/RHSA-2017:2682
- Bulletin de sécurité Red Hat RHSA-2017:2683 du 12 septembre 2017
  https://access.redhat.com/errata/RHSA-2017:2683
- Bulletin de sécurité Red Hat RHSA-2017:2704 du 13 septembre 2017
  https://access.redhat.com/errata/RHSA-2017:2704
- Bulletin de sécurité Red Hat RHSA-2017:2705 du 13 septembre 2017
  https://access.redhat.com/errata/RHSA-2017:2705
- Bulletin de sécurité Red Hat RHSA-2017:2706 du 13 septembre 2017
  https://access.redhat.com/errata/RHSA-2017:2706
- Bulletin de sécurité Red Hat RHSA-2017:2707 du 13 septembre 2017
  https://access.redhat.com/errata/RHSA-2017:2707
- Bulletin de sécurité Red Hat RHSA-2017:2731 du 14 septembre 2017
  https://access.redhat.com/errata/RHSA-2017:2731
- Bulletin de sécurité Red Hat RHSA-2017:2732 du 14 septembre 2017
  https://access.redhat.com/errata/RHSA-2017:2732
- Référence CVE CVE-2017-1000251
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000251
- Référence CVE CVE-2017-7895
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7895

Gestion détaillée du document

13 septembre 2017 version initiale.

14 septembre 2017 ajout de bulletins et mise à jour des systèmes affectés.