

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les noyaux Linux de Red Hat

Gestion du document

Référence	CERTFR-2016-AVI-275
Titre	Multiples vulnérabilités dans les noyaux Linux de Red Hat
Date de la première version	11 août 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Red Hat RHSA-2016:1581-1 du 09 août 2016 Bulletin de sécurité Red Hat RHSA-2016:1277-1 du 23 juin 2016 Bulletin de sécurité Red Hat RHSA-2016:1301-1 du 23 juin 2016 Bulletin de sécurité Red Hat RHSA-2016:1489-1 du 26 juillet 2016 Bulletin de sécurité Red Hat RHSA-2016:1341-1 du 27 juin 2016 Bulletin de sécurité Red Hat RHSA-2016:1406-1 du 12 juillet 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

- Red Hat Enterprise Linux Server AUS (v. 6.4), avec un noyau antérieur à la version 2.6.32-358.72.1
- Red Hat Enterprise Linux Desktop (v. 7), avec un noyau antérieur à la version 3.10.0-327.22.2
- Red Hat Enterprise Linux HPC Node (v. 7), avec un noyau antérieur à la version 3.10.0-327.22.2
- Red Hat Enterprise Linux HPC Node EUS (v. 7.2), avec un noyau antérieur à la version 3.10.0-327.22.2
- Red Hat Enterprise Linux Server (v. 7), avec un noyau antérieur à la version 3.10.0-327.22.2
- Red Hat Enterprise Linux Server AUS (v. 7.2), avec un noyau antérieur à la version 3.10.0-327.22.2
- Red Hat Enterprise Linux Server EUS (v. 7.2), avec un noyau antérieur à la version 3.10.0-327.22.2
- Red Hat Enterprise Linux Workstation (v. 7), avec un noyau antérieur à la version 3.10.0-327.22.2
- Red Hat Enterprise Linux for Real Time (v. 7), avec un noyau antérieur à la version 3.10.0-327.22.2.rt56.230
- Red Hat Enterprise Linux Server EUS (v. 6.7.z), avec un noyau antérieur à la version 2.6.32-573.32.1

- Red Hat Enterprise MRG v2 pour Red Hat Enterprise Linux (version 6), avec un noyau antérieur à la version 3.10.0-327.rt56.190
- Red Hat Enterprise Linux Desktop (v. 6), avec un noyau antérieur à la version 2.6.32-642.3.1
- Red Hat Enterprise Linux HPC Node (v. 6), avec un noyau antérieur à la version 2.6.32-642.3.1
- Red Hat Enterprise Linux Server (v. 6), avec un noyau antérieur à la version 2.6.32-642.3.1
- Red Hat Enterprise Linux Workstation (v. 6), avec un noyau antérieur à la version 2.6.32-642.3.1

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *les noyaux Linux de Red Hat*. 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 Red Hat RHSA-2016:1581-1 du 09 août 2016
<https://rhn.redhat.com/errata/RHSA-2016-1581.html>
- Bulletin de sécurité Red Hat RHSA-2016:1277-1 du 23 juin 2016
<https://rhn.redhat.com/errata/RHSA-2016-1277.html>
- Bulletin de sécurité Red Hat RHSA-2016:1301-1 du 23 juin 2016
<https://rhn.redhat.com/errata/RHSA-2016-1301.html>
- Bulletin de sécurité Red Hat RHSA-2016:1489-1 du 26 juillet 2016
<https://rhn.redhat.com/errata/RHSA-2016-1489.html>
- Bulletin de sécurité Red Hat RHSA-2016:1341-1 du 27 juin 2016
<https://rhn.redhat.com/errata/RHSA-2016-1341.html>
- Bulletin de sécurité Red Hat RHSA-2016:1406-1 du 12 juillet 2016
<https://rhn.redhat.com/errata/RHSA-2016-1406.html>
- Référence CVE CVE-2016-3707
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3707>
- Référence CVE CVE-2016-4565
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4565>
- Référence CVE CVE-2016-8767
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8767>

Gestion détaillée du document

11 août 2016 version initiale.

Conditions d'utilisation de ce document : <http://cert.ssi.gouv.fr/cert-fr/apropos.html>
Dernière version de ce document : <http://cert.ssi.gouv.fr/site/CERTFR-2016-AVI-275>
