



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
*Agence nationale de la sécurité
des systèmes d'information*
CERTA

Paris, le 18 juillet 2011
N° CERTA-2011-AVI-393

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Mise à jour du noyau Red Hat

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-393>

Gestion du document

Référence	CERTA-2011-AVI-393
Titre	Mise à jour du noyau Red Hat
Date de la première version	18 juillet 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Red Hat RHSA-2011:0927-1 du 15 juillet 2011
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

- Déni de service à distance ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

2 Systèmes affectés

- Red Hat Enterprise Linux (v. 5 server) ;
- Red Hat Enterprise Linux Desktop (v. 5 client) ;
- Red Hat Enterprise Linux EUS (v. 5.6.z server) ;
- Red Hat Enterprise Linux Long Life (v. 5.6 server).

3 Résumé

Plusieurs vulnérabilités affectant le noyau Linux Red Hat ont été corrigées par la mise à jour RHSA-2011:0927.

4 Description

Un total de 15 vulnérabilités ont été corrigées par la mise à jour *Red Hat Linux* RHTSA-2011:0927 du 15 juillet 2011.

Parmi celles-ci, six sont marquées comme importantes et concernent des vulnérabilités de type déni de service et/ou élévation de privilèges. Quatre sont classifiées comme ayant un impact modéré. Elles ont pour conséquence un déni de service. Les cinq dernières sont considérées comme ayant un impact faible et correspondent à des fuites d'informations ou des dénis de service.

5 Solution

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

6 Documentation

- Bulletin de sécurité Red Hat RHTSA-2011:0927 du 15 juillet 2011 :
<http://rhn.redhat.com/errata/RHTSA-2011-0927.html>
- Référence CVE CVE-2011-4649 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4649>
- Référence CVE CVE-2011-0695 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0695>
- Référence CVE CVE-2011-0711 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0711>
- Référence CVE CVE-2011-1044 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1044>
- Référence CVE CVE-2011-1182 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1182>
- Référence CVE CVE-2011-1573 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1573>
- Référence CVE CVE-2011-1576 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1576>
- Référence CVE CVE-2011-1593 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1593>
- Référence CVE CVE-2011-1745 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1745>
- Référence CVE CVE-2011-1746 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1746>
- Référence CVE CVE-2011-1776 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1776>
- Référence CVE CVE-2011-1936 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1936>
- Référence CVE CVE-2011-2022 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2022>
- Référence CVE CVE-2011-2213 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2213>
- Référence CVE CVE-2011-2492 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2492>

Gestion détaillée du document

18 juillet 2011 version initiale.