

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans logrotate

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-189>

Gestion du document

Référence	CERTA-2011-AVI-189
Titre	Vulnérabilités dans logrotate
Date de la première version	05 avril 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité RHSA-2011:0407 de Red Hat du 31 mars 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

- Exécution de code arbitraire ;
- déni de service ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Red Hat Enterprise Linux Desktop v.6 ;
- Red Hat Enterprise Linux HPC Node v.6 ;
- Red Hat Enterprise Linux Server v.6 ;
- Red Hat Enterprise Linux Workstation v.6.

3 Résumé

Plusieurs vulnérabilités pouvant conduire à un déni de service, une exécution de code arbitraire et une atteinte à la confidentialité des données ont été découvertes dans *logrotate*.

4 Description

Plusieurs vulnérabilités ont été corrigées dans *logrotate*. La première permet à une personne malintentionnée d'exécuter du code arbitraire sous l'identité du propriétaire du processus `logrotate` (`root`, par défaut) (CVE-2011-1154). La deuxième rend possible le déclenchement d'un déni de service (CVE-2011-1098). La troisième permet à un utilisateur malintentionné de porter atteinte à la confidentialité des données (CVE-2011-1155).

5 Solution

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

6 Documentation

- Bulletin de sécurité RedHat RHSA-2011:0407 du 31 mars 2011 :
<http://rhn.redhat.com/errata/RHSA-2011-0407.html>
- Référence CVE CVE-2011-1098 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1098>
- Référence CVE CVE-2011-1154 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1154>
- Référence CVE CVE-2011-1155 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1155>

Gestion détaillée du document

05 avril 2011 version initiale.