

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Red Hat Network Satellite

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-525>

Gestion du document

Référence	CERTA-2011-AVI-525
Titre	Vulnérabilités dans Red Hat Network Satellite
Date de la première version	19 septembre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Red Hat RHSA-2011:1299-1 du 15 septembre 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

- Injection de code indirecte à distance ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Red Hat Network Satellite version 5.4 pour RHEL 5 ;
- Red Hat Network Satellite version 5.4 pour RHEL 6.

3 Résumé

Des vulnérabilités de type injection de code indirecte à distance (XSS) ont été identifiées, ainsi qu'une vulnérabilité permettant, à partir de la page de connexion, de rediriger l'utilisateur vers une page Web arbitraire.

4 Description

- Ces vulnérabilités peuvent être utilisées par une personne intentionnée distante pour :
- effectuer des injections de code indirecte à distance (XSS) ;

- rediriger l'utilisateur vers une page Web arbitraire suite à une connexion réussie.

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-2011:1299-1 du 19 septembre 2011 :
<http://rhn.redhat.com/errata/RHSA-2011-1299.html>
- Référence CVE CVE-2011-1594 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1594>
- Référence CVE CVE-2011-2919 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2919>
- Référence CVE CVE-2011-2920 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2920>
- Référence CVE CVE-2011-2927 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2927>
- Référence CVE CVE-2011-3344 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3344>

Gestion détaillée du document

19 septembre 2011 version initiale.