

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Splunk

---

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-587>

---

### Gestion du document

|                             |  |
|-----------------------------|--|
| Référence                   | CERTA-2011-AVI-587   |
| Titre                       | Vulnérabilités dans Splunk   |
| Date de la première version | 21 octobre 2011  |
| Date de la dernière version | –  |
| Source(s)                   | Bulletins de sécurité Splunk SPL-42471 et SPL-42474 du 19 octobre 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 ;
- injection de code indirecte à distance.

## 2 Systèmes affectés

*Splunk* versions 4.0 à 4.2.3 (incluses).

## 3 Résumé

Deux vulnérabilités dans *Splunk* permettent de réaliser un déni de service et d'injecter du code indirectement à distance.

## 4 Description

Deux vulnérabilités ont été découvertes dans le composant *Splunk Web* de *Splunk*. La première permet d'injecter du code indirectement, en incitant un utilisateur à suivre un lien spécifiquement constitué. La seconde permet d'épuiser les ressources du système.

## **5 Solution**

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

## **6 Documentation**

- Bulletins de sécurité Splunk SPL-42471 et SPL-42474 du 19 octobre 2011 :  
<http://www.splunk.com/view/SP-CAAAGGH>

## **Gestion détaillée du document**

**21 octobre 2011** version initiale.