

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Splunk 4.1.5

---

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-2010-AVI-445>

---

### Gestion du document

Référence	CERTA-2010-AVI-445
Titre	Vulnérabilités dans Splunk 4.1.5
Date de la première version	20 septembre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Splunk SP-CAAAFQ6 du 09 septembre 2010
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

- Contournement de la politique de sécurité ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

## 2 Systèmes affectés

*Splunk* versions 4.0 à 4.1.4.

## 3 Résumé

Deux vulnérabilités corrigées dans *Splunk* permettent à un attaquant d'élever ses privilèges et d'accéder frauduleusement à des informations confidentielles.

## 4 Description

Une erreur dans l'analyseur syntaxique de documents XML permet à un attaquant authentifié d'élever ses privilèges et d'accéder à des informations confidentielles.

La clé de session peut être obtenue par une personne malintentionnée en forçant un utilisateur à visiter une page malveillante spécialement construite. Cette clé peut alors être réutilisée pour obtenir les mêmes privilèges.

## **5 Solution**

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

## **6 Documentation**

- Bulletin de sécurité Splunk SP-CAAAFQ6 du 09 septembre 2010  
<http://www.splunk.com/view/SP-CAAAFQ6>
- Référence CVE CVE-2010-3322 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3322>
- Référence CVE CVE-2010-3323 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3323>

## **Gestion détaillée du document**

**20 septembre 2010** version initiale.