

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-700>

Gestion du document

Référence	CERTA-2011-AVI-700
Titre	Vulnérabilités dans Splunk
Date de la première version	16 décembre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Splunk SP-CAAAGMM du 12 décembre 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 à distance ;
- atteinte à la confidentialité des données ;
- injection de code indirecte à distance.

2 Systèmes affectés

Splunk 4.x.

3 Résumé

Plusieurs vulnérabilités ont été corrigées dans Splunk. Elles permettent d'exécuter du code arbitraire, de faire de l'injection de code indirecte à distance et de porter atteinte à la confidentialité des données.

4 Description

Trois vulnérabilités ont été corrigées dans les composants Splunk Web et Splunkd HTTP Server. La première permet d'injecter du code indirectement, en incitant un utilisateur à suivre un lien spécifiquement conçu.

La seconde permet d'exécuter du code arbitraire à distance en incitant un administrateur à visiter une page Web spécialement constituée. La troisième permet à une personne malveillante d'explorer l'arborescence du serveur Splunk en portant ainsi atteinte à la confidentialité des données.

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-CAAAGMM du 12 décembre 2011 :
<http://www.splunk.com/view/SP-CAAAGMM>

Gestion détaillée du document

16 décembre 2011 version initiale.