Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 12 mars 2012
N° CERTA-2012-AVI-131

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Splunk

Gestion du document

Référence	CERTA-2012-AVI-131
Titre	Vulnérabilité dans Splunk
Date de la première version	12 mars 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Splunk SP-CAAAGTK du 05 mars 2012
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.

2 Systèmes affectés

Splunk versions antérieures à 4.3.1.

3 Résumé

Une vulnérabilité a été corrigée dans Splunk, qui peut être exploitée pour une injection de code indirecte à distance.

4 Description

Une vulnérabilité a été corrigée dans Splunk. Dans certaines situations, un attaquant peut l'exploiter et réaliser une injection de code indirecte à distance.

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-CAAAGTK du 05 mars 2012 :
http://www.splunk.com/view/SP-CAAAGTK

Gestion détaillée du document

12 mars 2012 version initiale.