

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans ArcSight Connector Appliance

---

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-398>

---

### Gestion du document

Référence	CERTA-2011-AVI-398
Titre	Vulnérabilité dans ArcSight Connector Appliance
Date de la première version	19 juillet 2011
Date de la dernière version	–
Source(s)	Note de vulnérabilité de l'US-CERT VU#122054 du 15 juillet 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.

## 2 Systèmes affectés

HP ArcSight Connector Appliance version 6.0.0.60023.2.

## 3 Résumé

ArcSight Connector Appliance est vulnérable à une injection de code indirecte à distance.

## 4 Description

Le module *Windows Event Log SmartConnector* inclus dans *ArcSight Connector Appliance* est vulnérable à une injection de code indirecte à distance lors de la génération de rapport.

## **5 Solution**

Contactez l'éditeur pour l'obtention du correctif permettant de mettre à jour en version 6.1.

## **6 Documentation**

- Note de vulnérabilité de l'US-CERT VU#122054 du 15 juillet 2011 :  
<http://www.kb.cert.org/vuls/id/122054>
- Référence CVE CVE-2011-0770 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0770>

## **Gestion détaillée du document**

**19 juillet 2011** version initiale.