

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans CA Arcot WebFort Versatile Authentication Server

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-256>

Gestion du document

Référence	CERTA-2011-AVI-256
Titre	Vulnérabilités dans CA Arcot WebFort Versatile Authentication Server
Date de la première version	27 avril 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité CA technologies CA20110426-01
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

CA Arcot WebFort Versatile Authentication Server (VAS) antérieur à la version 6.2.5.

3 Résumé

Deux vulnérabilités permettant à un utilisateur malintentionné d'injecter indirectement du code à distance ont été identifiées dans *CA Arcot WebFort Versatile Authentication Server*.

4 Description

Deux vulnérabilités ont été découvertes dans *CA Arcot WebFort Versatile Authentication Server*. Elle permettent à une personne malintentionnée d'injecter indirectement du code 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 CA technologies du 26 avril 2011 :
<https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID={A71F5839-D214-4719-B918-4476E4537998}>
- Référence CVE CVE-2011-1825 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1825>
- Référence CVE CVE-2011-1826 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1826>

Gestion détaillée du document

27 avril 2011 version initiale.