



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 avril 2011
N° CERTA-2011-AVI-229

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans CA Total Defense

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-229>

Gestion du document

Référence	CERTA-2011-AVI-229
Titre	Vulnérabilités dans CA Total Defense
Date de la première version	15 avril 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité CA20110413-01 du 13 avril 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 ;
- injection SQL ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

CA Total Defense version r12.

3 Résumé

Des vulnérabilités dans CA Total Defense permettent l'exécution de code arbitraire à distance ainsi que des injections SQL.

4 Description

Plusieurs vulnérabilités ont été découvertes dans *CA Total Defense* :

- un mauvais filtrage des paramètres de certaines requêtes permet d'effectuer diverses injections SQL (CVE-2011-1653);
- les paramètres utilisés lors d'un dépôt de fichier ne sont pas correctement filtrés, ce qui peut mener à une exécution de code arbitraire à distance (CVE-2011-1654);
- certaines informations sensibles ne sont pas correctement protégées, ce qui permet la récupération d'identifiants de connexion (CVE-2011-1655).

5 Solution

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

6 Documentation

- Bulletin de sécurité CA20110413-01 du 13 avril 2011 :
<https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID={CD065CEC-AFE>
- Référence CVE CVE-2011-1653 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1653>
- Référence CVE CVE-2011-1654 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1654>
- Référence CVE CVE-2011-1655 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1655>

Gestion détaillée du document

15 avril 2011 version initiale.