

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans EMC Captiva eInput

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-418>

Gestion du document

Référence	CERTA-2011-AVI-418
Titre	Multiples vulnérabilités dans EMC Captiva eInput
Date de la première version	29 juillet 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité EMC ESA-2011-024 du 26 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

- Déni de service ;
- atteinte à la confidentialité des données ;
- injection de code indirecte à distance.

2 Systèmes affectés

EMC Captiva eInput 2.x.

3 Résumé

Deux vulnérabilités dans EMC Captiva eInput ont été corrigées. Elles permettent à un utilisateur malveillant de conduire des attaques par injection de code indirecte, d'accéder à des données protégées, ou de porter atteinte à la disponibilité du système.

4 Description

Deux vulnérabilités ont été identifiées dans EMC Captiva eInput :

- certaines entrées non spécifiées ne sont pas correctement traitées avant d'être retournées à l'utilisateur, et permettent ainsi une injection de code indirecte à distance ;
- Une erreur dans une fonction EMC Captiva eInput `ActiveX` permet un accès distant à des données locales. Un déni de service peut aussi être conduit via ce vecteur.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). La mise à jour EMC Captiva eInput 2.1.1.37 corrige ces problèmes.

6 Documentation

- Bulletin de sécurité EMC ESA-2011-024 du 26 juillet 2011 :
<http://archives.neohapsis.com/archives/bugtraq/2011-07/att-0178/ESA-2011-024.txt>
- Référence CVE CVE-2011-1743 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1743>
- Référence CVE CVE-2011-1744 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1744>

Gestion détaillée du document

29 juillet 2011 version initiale.