Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 juin 2012
N° CERTA-2012-AVI-349

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans IBM System Storage DS Storage Manager

Gestion du document

Référence	CERTA-2012-AVI-349
Titre	Vulnérabilités dans IBM System Storage DS Storage Manager
Date de la première version	22 juin 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité IBM H206045 du 15 juin 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

- Exécution de code arbitraire à distance ;
- injection de code indirecte à distance.

2 Systèmes affectés

- DS4100 (FAStT100) Dual-Controller Storage Server, type 1724 ;
- DS4200 Storage Server, type 1814 ;
- DS4300 (FAStT600) Dual-Controller et Turbo Storage Server, type 1722 ;
- DS4400 (FAStT700) Storage Server, type 1742 ;
- DS4500 (FAStT900) Storage Server, type 1742 ;
- DS4700 Storage Server, type 1814 ;
- DS4700 Storage Server, type 1814 (alimentations DC);
- DS4800 Storage Server, type 1814 ;
- IBM System Storage DCS3700 Storage Subsystem, type 1818, modèle 80C ;
- IBM System Storage DS3200, type 1726 ;
- IBM System Storage DS3300, type 1726 ;
- IBM System Storage DS3400, type 1726 ;

- IBM System Storage DS3512, type 1746 ;
- IBM System Storage DS3524, type 1746 ;
- IBM System Storage DS3950 Express, type 1814 ;
- IBM System Storage DS5020 Disk Controller (1814-20A) ;
- IBM System Storage DS5100 Storage Controller, type 1818 ;
- IBM System Storage DS5300 Storage Controller, type 1818.

3 Résumé

Deux vulnérabilité ont été corrigées par IBM pour les produits *Storage Server*. La première (CVE-2012-2171) permet à un utilisateur malveillant d'injecter et d'exécuter du code SQL arbitraire à distance. La seconde (CVE-2012-2172) permet à un attaquant de réaliser de l'injection de code indirecte à distance.

4 Solution

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

5 Documentation

- Bulletin de sécurité IBM H206045 du 15 juin 2012 :
  https://www-304.ibm.com/connections/blogs/PSIRT/entry/secbulletin_stg-storage_cve-2012-2171_cve-2012-2172?lang=en_gb
  http://www-947.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5090850&brandind=5000028
- Référence CVE CVE-2012-2171 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2171
- Référence CVE CVE-2012-2172 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2172

Gestion détaillée du document

22 juin 2012 version initiale.