Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 mars 2012
N° CERTA-2012-AVI-159

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Dell PowerVaul ML6000

Gestion du document

Référence	CERTA-2012-AVI-159
Titre	Multiples vulnérabilités dans Dell PowerVaul ML6000
Date de la première version	21 mars 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité VU#913483
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

- Versions antérieures au firmware *A20-00 (590G.GS00100)*.

3 Résumé

De multiples vulnérabilités ont été corrigées dans le produit *Dell PowerVaul ML6000*. L'exploitation de ces vulnérabilités pouvait conduire à une prise de contrôle du serveur.

4 Description

Trois vulnérabilités ont été corrigées dans le produit *Dell PowerVaul ML6000*. La permière est accessible par un utilisateur non authentifié, la faille est de type « inclusion de fichier » et touche la page « logShow.htm ». La deuxième permet une injection de code dite *XSS* dans la page « checkQKMProg.html ». La troisième touche la

page « saveRestore.htm » (via une méthode *POST*) et permet une exécution de commandes arbitaires avec les droits de l'utilisateur « root ».

5 Solution

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

6 Documentation

- Note de vulnérabilité de l'US-CERT VU#913483 du 19 mars 2012 :
  http://www.kb.cert.org/vuls/id/913483

Gestion détaillée du document

21 mars 2012 version initiale.