Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 mars 2012
N° CERTA-2012-AVI-158

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Aruba Networks

Gestion du document

Référence	CERTA-2012-AVI-158
Titre	Vulnérabilités dans Aruba Networks
Date de la première version	20 mars 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Aruba Networks AID-031912
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.

2 Systèmes affectés

- Versions antèrieures à ArubaOS 5.0.4.2 ;
- Versions antèrieures à ArubaOS 6.0.2.1 ;
- Versions antèrieures à ArubaOS 6.1.2.4.

3 Résumé

Deux vulnérabilités ont été corrigées dans *ArubaOS*. L'exploitation de ces vulnérabilités pouvait conduire à une prise de contrôle totale sur le système distant.

4 Description

La première vulnérabilité est située dans l'interface Web de diagnostic réseau. Une injection de commande à distance peut être utilisée pour exécuter des actions avec le compte utilisateur « root ». La deuxième vulnérabilité affecte le composant *EAP-TLS 802.1X* et peut autoriser l'accès au réseau à un utilisateur non désiré.

5 Solution

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

6 Documentation

– Bulletin de sécurité Aruba Networks AID-031912 du 19 mars 2012 :
http://www.arubanetworks.com/support/alerts/aid-031912.asc

Gestion détaillée du document

20 mars 2012 version initiale.