NVC NETWORK VALUE COMPONENTS

2008 年 3 月 18 日

お客様各位

株式会社ネットワークバリューコンポネンツ

Aruba Mobility Controller シリーズにおける脆弱性に関するお知らせ

記

Aruba Networks 社より Aruba Mobility Controller の内部に影響する脆弱性が発見されたとの連絡が入りました。本脆弱性によるリスクを最小限にするため、システムのアップグレードに必要な時間を見越して、一般的な公表を行う前に先行してお客様にご連絡しております。
Bugtraq アドバイザリーによる公示は 2008 年 5 月 14 日を予定しています。この勧告では既存システムの保護のため脆弱性の詳細については記述致しません。

本脆弱性につきましては、以下の点が報告されております。

- Aruba Mobility Controller の WebUI に対してクロスサイトスクリプティングを実施されることによって、管理情報を不正に取得される可能性がある
- TACACS 認証をマネージメントアクセスに使用している場合に管理権限を不正に取得される可能性がある

本脆弱性は、Aruba Mobility Controller を使用している全てのユーザに影響致します。
この問題を回避するために、直ちにパッチ版にアップグレードすることをお奨め致します。
また、パッチ版にアップグレードするまでは不用意にマネージメントアクセスを許可しないように ACL を設定することでリスクを低減することも可能です。ただ、最終的な対策としてはパッチ版のアップグレードのみとなりますのでご注意ください。

1. 対象機器：
   Aruba Mobility Controller
2. 対象機能：
   Aruba Mobility Controller の WebUI 管理機能、TACACS 認証機能
3. 対策方法：
   弊社担当までお問い合わせください。下記のものを用意しております。
   - 各 Mobility Controller 用パッチ版 OS
   - OS リリースノート
   - OS 適用手順書
   - Aruba マネージメントアクセス制限設定手順書

＊ TACACS 認証についての脆弱性は ArubaOS3.1 が対象です。

その他、本件につきましては弊社担当営業、もしくはサポート窓口までお問い合わせいただきますようお願い申し上げます。

以　上