TD61-2669B
HCVU000000004
2005 年 8 月 12 日
日立電線株式会社

WirelessIP5000:ネットワークアクセスに関する脆弱性について

1. 脆弱性の概要

WirelessIP5000 において下記の複数の脆弱性が報告されています。(JVN#76659792)

(a) ドキュメントに無いアクセス可能な TCP ポート
概要：TCP3390 番ポートを用いて不正アクセスが可能
影響：第三者が侵害作業のための情報収集に悪用する可能性がある

(b) SNMP に関する脆弱性
概要：任意のコミュニティ名にて SNMP アクセスが可能
影響：第三者が SNMP プロトコルを利用し設定変更することが可能

(c) HTTP サーバ認証
概要：工場出荷の設定において認証されないユーザが HTTP サーバにアクセス可能
影響：第三者が Web ブラウザ等を用いて設定変更することが可能

(d) HTTP サーバにおける表示内容
概要:HTTP サーバ機能にて表示される内容に悪意を持った第三者が攻撃に利用できるような詳細情報が含まれている
影響：第三者が HTTP サーバに表示される情報を参照し、サービス運用妨害(DoS)攻撃に利用する可能性がある

(e) デフォルトパスワード
概要：工場出荷時に設定されている管理者のデフォルトパスワードが容易に想像し得る
影響：第三者が管理者用パスワードを悪用し内部の情報を参照する可能性がある

2. 参考情報

(1) JP Vendor Status Notes JVN#76659792
http://jvn.jp/jp/JVN%2376659792

3. 当社製品への影響

当社製品の本脆弱性に関する影響は下記の通りです。

製品名	Version	影響
WirelessIP5000	1.5.10 以前	本脆弱性(a)(b)(c)(d)(e)に該当
	2.0.0 以降	本脆弱性(a)(b)(e)に該当
	2.0.1 以降	本脆弱性(e)に該当

4. 対策

(a)(b)については提供されるパッチ(Version 2.0.1)以降をご使用下さい。
(c)(d)(e)については提供されるパッチ(Version 2.0.0)以降をご使用になるか運用時に適切なパスワードを設定して下さい。

5. 謝辞

本脆弱性情報についてご報告頂いた Shawn Merdinger 氏に深く感謝します。

以上