FutureNet RAシリーズにおけるSSLv3プロトコルの

暗号化データを解読される脆弱性(POODLE攻撃)について

[脆弱性情報]

弊社FutureNet RAシリーズは、JVNVU#98283300で報告されている「SSLv3 プロトコルに暗号化データを解読される脆弱性(POODLE攻撃)」に該当致します。

但し、本脆弱性の影響範囲についてはGUI利用時、並びにLDAP動作時のみとなります。

[対象製品]

FutureNet RA-1200

FutureNet RA-730

FutureNet RA-1100

FutureNet RA-630

※サポート終了製品はファームウェアのリリース予定がありませんので記載しておりません。

[参考情報]

http://jvn.jp/vu/JVNVU98283300/index.html

[対策方法]

本脆弱性の対策を施したファームウェアをダウンロードし、バージョンアップをおこなってください。

FutureNet RA-1200 Ver1.10.2で対応

FutureNet RA-730 Ver1.10.3で対応

※その他対象製品は順次対応予定

[該当している場合の回避方法]

- GUI利用時にはWebブラウザ側(TLSサポートのものに限る)でSSLv3の利用を禁止してください。
- LDAP利用時には本脆弱性対策済のLDAPサーバを利用するようにしてください。

[更新履歴]

2014/10/21 新規登録

2015/1/8 FutureNet RA-1200 Ver1.10.2で対応

2015/4/9 FutureNet RA-730 Ver1.10.3で対応