NVC NETWORK VALUE COMPONENTS

2004 年 4 月 23 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

TCP プロトコルの脆弱性による影響に関して

セキュリティ情報機関 NISCC より報告のあった TCP プロトコルの脆弱性(NISCC Vul/236929)が弊社製品に影響を及ぼすことが判明致しました。
本脆弱性の概要、影響範囲、および対処方法についてご案内致します。

記

1. 概要
   悪意のある第三者からの不正なパケットを受信することにより、正規のクライアントとの間の正常な通信を妨害される、あるいは、不正なデータを挿入 されるといった攻撃を受ける可能性があります。

2. 該当機種
   Riverstone 全般

3. 影響範囲
   TCP プロトコルによる通信を行う機能が、本脆弱性の影響を受けます。
   具体的には Telnet、Secure Shell、HTTP,BGP が該当します。
   TCP セッションを不正にリセットされることにより、正常な通信が妨げられる恐れがあります。また、正常な通信の途中で悪意のあるデータを挿入されることにより、不正な操作が行われる恐れがあります。

4. 回避策
   本脆弱性は RFC793 に従った全ての TCP 実装で共通のもので、現時点での回避方法はありません。
   但し、BGP 機能に関しては MD5 認証機能を設定頂くことにより本脆弱性に対する攻撃から回避することが可能です。

5. 対策
   BGP MD5 認証オプション
   下記のご質問について、下記設定で MD5 認証が適用されます。
   bgp set peer-host password <password>
   bgp set peer-group password <password>

   Specifies the password for MD5 access to a peer host.
   Password is case sensitive and can be 80 characters orless.

以　上