TD61-2593D
HCVU000000002
2005年5月25日
日立電線株式会社

TCPタイムスタンプオプションに関する脆弱性について

1．脆弱性の概要

RFC1323に規定されているTCP Timestamp Optionを使用し、IPアドレスおよびポート番号を偽装したTCPパケットを第三者が送りつけることによりPAWS(Protection Against Wrapped Sequence)機能を実装したTCPのコネクションが終了するサービス運用妨害(Denial of Service)攻撃の可能性が報告されています(JPCERT/CC REPORT 2005-05-25)。

2．参考情報

(1) JP Vendor Status Notes JVNVU#637934

TCP の実装に不正な値で内部タイマを更新する脆弱性

http://jvn.jp/cert/JVNVU%23637934/

(2) US-CERT Vulnerability Note VU#637934

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	OS名称	影響
Apresia®8000シリーズ	ApWare	本脆弱性に該当しません
Apresia®6000シリーズ	ApbWare	
Apresia®4000シリーズ	AEOS®	
Apresia®3000シリーズ	AEOS®, HSWWare Ver3,5	
Apresia®2000シリーズ	AEOS®, HSWWare Ver2,4	
GMXシリーズ	GMX-Ware1 GMX-Ware3 GMX-Ware4	
HSWシリーズ	HSWWare Ver2 HSWWare Ver3	

以上