TD61-2743
HCVU000000005
2005年10月31日
日立電線株式会社

OpenSSLの脆弱性について

1．脆弱性の概要

OpenSSLを利用したサーバにおいて特定のオプションを使用した場合、通信経路上で通信内容を改ざんされることにより､TLS/SSLのバージョンを強制的にSSL2.0の接続に変更される可能性が報告されています。

2．参考情報

(1) JP Vendor Status Notes JVN#23632449

OpenSSLにおけるバージョン・ロールバックの脆弱性

http://jvn.jp/jp/JVN%2323632449/index.html

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®	Ver6.10.00 以下では本脆弱性に該当します
Apresia®3000シリーズ	AEOS®	Ver6.10.00 以下では本脆弱性に該当します
	HSWWare Ver3 HSWWare Ver5	本脆弱性に該当しません
Apresia®2000シリーズ	AEOS®	Ver6.10.00 以下では本脆弱性に該当します
	HSWWare Ver2 HSWWare Ver4	本脆弱性に該当しません
GMXシリーズ	GMX-Ware1 GMX-Ware3 GMX-Ware4	本脆弱性に該当しません
HSWシリーズ	HSWWare Ver2 HSWWare Ver3	

4．回避策

本脆弱性の該当するバージョンのAEOSをご使用の際には、対策されたVer6.10.01以上をお使い下さい。

Ver6.10.01以上の適用が不可能な場合には、SSL2.0を使用せずSSL3.0あるいはTLS1.0のみを使用してHTTPS通信を行うことにより問題を回避することが出来ます。

以上