TD61-4361
HCVU000000008
2010 年 1 月 21 日
日立電線株式会社

SSL 及び TLS に関する脆弱性

1. 脆弱性の概要

Secure Sockets Layer (SSL) および Transport Layer Security (TLS) プロトコルの renegotiation 機能には、特定の条件において通信データの先頭に任意のデータを挿入できる脆弱性があります。結果として、通信を中継可能な第三者が HTTP リクエストを挿入してサーバに送信するなどの可能性があります。

2. 参考情報

SSL および TLS プロトコルに脆弱性
http://www.jpcert.or.jp/wr/2009/wr094401.html#3

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
Apresia18000 シリーズ	AMIOS	本脆弱性に該当しません。
Apresia16000 シリーズ	AMIOS	
Apresia8000 シリーズ	ApWare	
Apresia6000 シリーズ	ApbWare	
Apresia2000,3000,4000,5000,13000 シリーズ	AEOS6,AEOS7	本脆弱性に該当します。
Apresia13000 シリーズ	AEOS8	本脆弱性に該当しません。
ApresiaLight	APL-Ware	
XGMC シリーズ	-	
GMC シリーズ	-	
GMX シリーズ	-	
eWAVE シリーズ	-	
BMC/OMC シリーズ	-	
FEMX シリーズ	-	
GMA シリーズ	-	

注) 不正に端末を認証させる等、本脆弱性を利用して Apresia の運用に影響を与える方法は見つかっておりません。

4. 回避策

回避策としては、MAC 認証と Web 認証を併用する等により信頼できない装置からのアクセスをフィルタする方法がございます。

根本的な対策については、対策ファームウェアのリリースをお待ちください。

以上