Cente Technical Information

発行番号	006-0002	Rev	第1版	発行日	2012/07/05
題名	不正なパディング長のデータを受信したとき、不正なメモリアクセスが発生することがある				
情報分類	障害情報				
適用製品	・Cente Compact SSL Ver.1.00				
関連資料	なし				

【該当するユーザ環境】
Cente Compact SSL Ver.1.00を使用しているユーザ。

【障害内容】
SSLのメッセージ単位である1レコードの最後には任意長のパディングと、パディング長がセットされています。このパディング長が不正な場合、正しくエラーとして破棄できずに不正なメモリアクセスが発生する可能性があります。

【発生理由】
パディングを除いた実際のデータ部分を取得するため、パディング長で示されている長さだけレコードを短くする処理があります。ここで、パディング長が不正（レコード長より長い）場合に長さが負の数になりますが、長さを符号なし整数で保持していたため、正しくエラー処理できていませんでした。環境によっては、ビルド時にこの部分がエラーまたはワーニングとなる場合もあります。

【回避方法】
ソースコードを修正し、不正なパディング長の場合は正しくエラー処理できるようにする必要があります。
（改変箇所については、営業担当またはsupport@cente.jpまでお問い合わせください。）

以上