Cente Technical Information

発行番号	001-0059	Rev	第1版	発行日	2017/01/09
題名	TCP切断API実行後、一定時間内にデータ受信があった場合の意図しないメモリ書き込みについて				
情報分類	障害情報				
適用製品	・Cente TCP/IPv4 Ver.1.00 - Ver.1.35 ・Cente TCP/IPv4 SNMPv2 Ver.1.00 - Ver.2.22 ・Cente TCP/IPv4 SNMPv3 Ver.1.00 - Ver.2.22 ・Cente IPv6 Ver.1.00 - Ver.1.45 ・Cente IPv6 SNMPv2 Ver.1.00 - Ver.2.22 ・Cente IPv6 SNMPv3 Ver.1.00 - Ver.2.22				
関連資料	なし				

【該当するユーザ環境】
TCPを使用しており、自分から切断を実行した後に通信相手からデータを受信する可能性がある環境。

【障害内容】
TCPが使用する受信バッファは、TCPのAPIを呼ぶアプリケーション側で確保してTCPに渡します(BSDソケットAPI使用時はミドルウエア内部に確保されています)。
TCP切断APIを実行した後、そのメモリ領域は解放したり次のTCP接続に使用するなど、別の目的で使用することが可能です。
しかし、TCP切断APIを実行した直後に通信相手からデータを受信すると、それまで受信バッファとして指定されていたメモリ領域にデータを書き込んでいました。

そのため、アプリケーションによっては以下のような症状が発生する場合があります。
・メモリ破壊(受信バッファを解放したり、別目的で使用している場合)
・次のTCP接続の受信データに上書き(静的なメモリを繰り返し使用している場合)

【発生理由】
TCP切断APIから返ってきた後も、相手からFINやFINの再送を受信してACKを返すためにTCP接続を短い時間(デフォルト0.5秒)継続しています。このタイミングで相手からデータを受信した場合、アプリケーション側で確保した受信バッファのメモリアドレスを保持しており、このアドレスにデータを書き込んでいました。

【回避方法】
以下のいずれかの方法で回避することが可能です。
・運用で回避:TCP切断APIから返ってきた後、TCP_TIMEWAIT(デフォルト0.5秒)だけ受信バッファの解放や次のTCPソケット作成を待ってください。
・ソースコードの修正:TCP切断APIから返った後にデータを受信した場合、受信バッファに書き込まずに破棄するようにします。
(詳細については、営業担当またはsupport@cente.jpまでお問い合わせください。)

以上