

# Cente Technical Information

発行番号	001-0036	Rev	第1版	発行日	2011/12/09
題名	オプションフィールドの長さが不正なTCPパケットを受信すると無限ループが発生する				
情報分類	障害情報				
適用製品	<ul style="list-style-type: none"><li>・Cente TCP/IPv4 Ver.1.00 - Ver.1.32</li><li>・Cente TCP/IPv4 SNMPv2 Ver.1.00 - Ver.2.12</li><li>・Cente TCP/IPv4 SNMPv3 Ver.2.00 - Ver.2.12</li><li>・Cente IPv6 Ver.1.00 - Ver.1.42</li><li>・Cente IPv6 SNMPv2 Ver.1.00 - Ver.2.12</li><li>・Cente IPv6 SNMPv3 Ver.2.00 - Ver.2.12</li></ul>				
関連資料	なし				
<p><b>【該当するユーザ環境】</b> 適用製品上でTCP通信を使用している全てのユーザ。</p> <p><b>【障害内容】</b> TCPヘッダには各種オプション情報を相手に通知するためのオプションフィールドがあります。TCPソケットがオープンしている状態のとき、不正なオプション内容を持ったTCPパケットを受信すると、その処理部分で無限ループが発生してしまい、以後一切通信できない状態になります。</p> <p><b>【発生理由】</b> TCPオプションフィールドに含まれる個々のオプションは、以下のような形になっています。</p> <p><b>[種別][長さ][内容]</b> 対応していないオプションを受信した場合、上記の[長さ]フィールドで指定された長さだけスキップして、次のオプション解釈に進みます。ここで、[長さ]フィールドが0だった場合、スキップできずにその場で無限ループが発生していました。</p> <p><b>【回避方法】</b> ・ソースコードを修正し、不正なオプションだった場合は直ちに処理を終了させる。 (変更箇所については、営業担当またはsupport@cente.jpまでお問い合わせください。)</p> <p style="text-align: right;">以上</p>					