FTP クライアントインスペクタ

FTP クライアントインスペクタの概要

タイプ	インスペクタ（パッシブ）
使用方法	検査
インスタンス タイプ	マルチトン
その他のインスペクタが必要	`ftp_server`、`stream_tcp`
有効	`true`

File Transfer Protocol（FTP）は、TCP/IP を介してクライアントとサーバー間でファイルを転送するために使用されるネットワークプロトコルです。クライアントとサーバーが接続を確立すると、クライアントはサーバーにコマンドを発行してファイルをサーバーにアップロードするか、またはサーバーからファイルをダウンロードし、サーバーからの応答を解釈します。

`ftp_client` インスペクタは、FTP コマンドチャネルの応答を確認して正規化します。

FTP コマンドチャネルバッファを指定すると、`ftp_client` インスペクタは FTP 応答コードとメッセージを解釈します。`ftp_client` インスペクタは、パラメータの正確性を適用し、FTP コマンド接続がいつ暗号化され、いつ FTP データチャネルが開かれるかを決定します。

FTP クライアントインスペクタのパラメータ

bounce

クライアントが発行した `ftp port` コマンド内のホスト情報を確認して FTP バウンスを確認するかどうかを指定します。`bounce` が `true` に設定されている場合、`ftp port` コマンド内のホスト情報が設定されたクライアント IP アドレス、またはホスト情報と一致しておらず、ルール 125:8 が有効になっているときは、システムがアラートを生成し、インライン展開で問題のあるパケットをドロップします。これは、FTP バウンス攻撃を防ぎ、FTP データ チャネルの接続先がクライアントとは異なる FTP 接続を許可するために使用できます。

型：ブール値

有効な値：`true`、`false`

デフォルト値：`false`

ignore_telnet_erase_cmds

FTP コマンドチャネルを正規化するときに、消去文字（TNC EAC）と消去行文字（TNC EAL）の Telnet エスケープシーケンスを無視するかどうかを指定します。このパラメータは、FTP クライアントが Telnet 消去コマンドを処理する方法と一致するように設定する必要があります。通常、新しい FTP クライアントはこれらの Telnet エスケープシーケンスを無視しますが、レガシークライアントは通常、それらを処理します。`ignore_telnet_erase_cmds` パラメータが `false` の場合、インスペクタはルール 125:1 を使用してアラートを生成し、インライン展開で問題のあるパケットをドロップします。

型：ブール値

有効な値：`true`、`false`

デフォルト値：`false`

max_resp_len

クライアントが受け入れるすべての応答メッセージの最大長をバイト単位で指定します。FTP 応答のメッセージ（3 桁のリターンコードの後のすべて）がその長さを超え、ルール 125:6 が有効になっている場合、システムはアラートを生成し、インライン展開で問題のあるパケットをドロップします。これは、FTP クライアント内のバッファのオーバーフローのエクスプロイトを確認するために使用されます。

型：整数

有効な範囲：`0 〜 4,294,967,295 (max32)`

デフォルト値：`4,294,967,295`

telnet_cmds

FTP コマンドチャネルで Telnet コマンドを確認するかどうかを指定します。このようなコマンドがある場合は、FTP コマンドチャネルでの回避試行を示している可能性があります。

このパラメータのイベントを生成し、インライン展開で問題のあるパケットをドロップするには、ルール 125:1 を有効にします。

型：ブール値

有効な値：`true`、`false`

デフォルト値：`false`

FTP クライアントインスペクタのルール

`ftp_client` インスペクタのルールを有効にし、イベントを生成し、インライン展開では、違反パケットをドロップします。。

表 *1 : FTP* クライアントインスペクタのルール

GID:SID	ルール メッセージ
125:1	FTP コマンドチャネルの Telnet コマンド（TELNET cmd on FTP command channel）
125:6	FTP 応答メッセージが長すぎる（FTP response message was too long）
125:8	FTP バウンス試行（FTP bounce attempt）

FTP クライアントインスペクタの侵入ルールのオプション

`ftp_client` インスペクタには、侵入ルールのオプションはありません。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。