Telnet インスペクタ

Telnet インスペクタの概要

タイプ	インスペクタ（サービス）
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	`stream_tcp`
有効	`false`

Telnet は、TCP 上で 8 ビットバイトの通信チャネルを作成するアプリケーション層プロトコルです。Telnet は、ネットワーク仮想端末を使用して、クライアントとリモートホスト間の通信を行います。Telnet サーバーは TCP ポート 23 を使用します。

`telnet` インスペクタは、Telnet コマンドシーケンスとオプションのネゴシエーションを検出することで Telnet データバッファを正規化します。`telnet` インスペクタは、パケットから Telnet コマンドシーケンス（RFC 854）を除去します。`telnet` インスペクタは、Telnet 暗号化オプション（RFC 2946）を確認することで、暗号化された Telnet 接続を検出できます。

Telnet インスペクタのパラメータ

Telnet サービスの設定

binder インスペクタは、Telnet サービスの設定を定義します。詳細については、『バインダインスペクタの概要』を参照してください。

例：

```
[
    {
        "when": {
            "service": "telnet",
            "role": any
        },
        "use": {
            "type": "telnet"
        }
    }
]
```

ayt_attack_thresh

連続する Are You There（AYT） Telnet コマンドの最大数を指定します。telnet インスペクタは、ayt_attack_thresh 値を超える連続した AYT コマンドの数を検出し、アラートを生成します。ayt_attack_thresh パラメータは、Telnet の BSD 実装に関連する特定の脆弱性に対処します。ayt_attack_thresh パラメータを無効にするには、-1 を指定します。ルール 126:1 を有効にし、このパラメータのイベントを生成し、インライン展開では、違反パケットをドロップします。。

型：整数

有効な範囲：-1 ～ 2,147,483,647 (max31)

デフォルト値：-1

encrypted_traffic

暗号化された Telnet トラフィックを検出するかどうかを指定します。ルール 126:2 を有効にし、このパラメータのイベントを生成し、インライン展開では、違反パケットをドロップします。。

型：ブール値

有効な値：true、false

デフォルト値：false

normalize

Telnet トラフィックを正規化するかどうかを指定します。telnet インスペクタは、telnet エスケープシーケンスを除外することで、Telnet トラフィックを正規化します。有効な侵入ルール

で raw コンテンツパラメータが指定されている場合、このルールでは telnet インスペクタが作成した正規化された Telnet バッファを無視します。

型：ブール値

有効な値：true、false

デフォルト値：false

Telnet インスペクタのルール

telnet インスペクタを有効にし、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 : Telnet* インスペクタのルール

GID:SID	ルール メッセージ
126:1	連続した Telnet AYT コマンドがしきい値を超えている（consecutive Telnet AYT commands beyond threshold）
126:2	Telnet トラフィックが暗号化されている（Telnet traffic encrypted）
126:3	Telnet サブネゴシエーション開始コマンドにサブネゴシエーション終了がない（Telnet subnegotiation begin command without subnegotiation end）

Telnet インスペクタの侵入ルールのオプション

telnet インスペクタには、侵入ルールのオプションがありません。

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。