MMS インスペクタ

MMS 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`

IEC 61850 は、電力システムの通信プロトコルを定義する国際規格です。Manufacturing Message Specification（MMS）プロトコルは、IEC 61850 プロトコルの 1 つです。MMS を使用すると、さまざまな製造およびプロセス制御のデバイス間で遠隔監視制御・情報取得（SCADA）データをリアルタイムで転送できます。MMS プロトコルは、TCP ポート 102 を使用して、クライアントデバイスとサーバーデバイス間でメッセージを交換します。

`mms` インスペクタは、MMS トラフィックを検出および分析します。MMS メッセージには、1 つの TCP パケット内に複数のプロトコルデータユニット（PDU）、複数の TCP パケットに分割された 1 つの PDU、または 2 つのメッセージ設定の組み合わせが含まれる場合があります。`mms` インスペクタは、MMS トラフィックを正規化して完全な MMS メッセージをデバイスに提示します。

MMS プロトコルをデコードせずに、MMS メッセージの Snort 3 ルールを作成します。`mms` インスペクタは、MMS プロトコルをカプセル化する OSI レイヤーを分析し、ルールオプションを通じて特定の MMS プロトコルフィールドとデータコンテンツへのアクセスを提供します。

MMS ルールのオプションの詳細については、MMS インスペクタの侵入ルールのオプション（2 ページ） を参照してください。

MMS インスペクタのパラメータ

MMS サービスの設定

binder インスペクタは MMS 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": "mms"
        },
        "use": {
            "type": "mms"
        }
    }
]
```

MMS インスペクタのルール

mms インスペクタには関連付けられたルールがありません。

MMS インスペクタの侵入ルールのオプション

mms_data

検出カーソルの位置を MMS プロトコルデータユニット（PDU）の先頭に配置し、すべての OSI カプセル化層をバイパスします。侵入ルールに mms_data が含まれている場合、ルールの次のルールオプションは MMS PDU から処理を開始します。

シンタックス：mms_data;

例：

次のサンプル侵入ルールは、mms_data ルールオプションを設定します。mms_data ルールオプションは、検出カーソルを MMS PDU の先頭に配置し、その位置のバイトで Initiate-Request メッセージの値をチェックします。

```
alert tcp ( \
msg: "PROTOCOL-SCADA MMS Initiate-Request"; \
flow: to_server, established; \
mms_data; \
content:"|A8|", depth 1; \
```

```
sid:1000000; \
)
```

mms_func

提供された関数名または番号を、MMS要求または応答の`Confirmed Service`フィールドと比較します。MMS 機能の名前または番号が `Confirmed Service` と一致したときに警告します。

タイプ：文字列

シンタックス：`mms_func <function>;`

例：

次の侵入ルールの例では、`mms_func` ルールオプションを設定し、`Confirmed Service Request` サービスが提供された関数名と一致した場合に警告します。さらに、`mms_func` は、`Confirmed Service Request (0xA0)` メッセージで一致する高速パターンマッチング機能を有効にします。

```
alert tcp ( \
msg: "PROTOCOL-SCADA MMS svc get_name_list"; \
flow: to_server, established; \
content:"|A0|"; \
mms_func: get_name_list; \
sid:1000000; \
)
```

次のサンプル侵入ルールは、`mms_func` ルールオプションを設定し、`GetNameList` メッセージが関数番号と一致したときに警告します。

```
alert tcp ( \
msg: "PROTOCOL-SCADA MMS svc get_name_list"; \
flow: to_server, established; \
content:"|A0|"; \
mms_func:1; \
sid:1000001; \
)
```

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。