S7CommPlus インスペクタ

S7CommPlus 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`

S7CommPlus は、Siemens が開発した独自のプロトコルです。S7CommPlus は、Siemens S7 ファミリ製品のプログラマブル ロジック コントローラ間の通信を可能にします。

`s7commplus` インスペクタは、S7CommPlus トラフィックを検出して分析します。指定した S7CommPlus 関数と操作コードのヘッダーフィールドで警告を発し、S7CommPlus トラフィックでの攻撃を検出するように侵入ルールのオプションを設定できます。

S7CommPlusインスペクタを設定するためのベストプラクティス

ネットワークに有効になっているS7CommPlusデバイスが含まれていない場合は、トラフィックに適用するネットワーク分析ポリシーの `s7commplus` インスペクタを有効にする必要があります。

S7CommPlus インスペクタのパラメータ

S7CommPlus TCP ポートの設定

`binder` インスペクタは、S7CommPlus TCP ポート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": {
            "role": "server",
            "proto": "tcp",
            "ports": "102"
        },
        "use": {
            "type": "s7commplus"
        }
    },
    {
        "when": {
            "role": "any",
            "service": "s7commplus"
        },
        "use": {
            "type": "s7commplus"
        }
    }
]
```

（注） `s7commplus` インスペクタはパラメータを提供しません。

S7CommPlus インスペクタのルール

`s7commplus` 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 : S7CommPlus* インスペクタのルール

GID:SID	ルール メッセージ
149:1	S7commplus MBAP ヘッダーの長さが、指定した S7commplus 関数に必要な長さと一致しない（length in S7commplus MBAP header does not match the length needed for the given S7commplus function）
149:2	S7commplus プロトコル ID がゼロ以外になっている（S7commplus protocol ID is non-zero）
149:3	予約済み S7commplus 機能コードは使用中になっている（reserved S7commplus function code in use）

S7CommPlus インスペクタの侵入ルールのオプション

s7commplus インスペクタが検出したトラフィックに対する攻撃を識別するカスタム侵入ルールを作成するには、s7commplus キーワードを単体で使用するか、または組み合わせて使用します。設定可能なキーワードについては、許容範囲内の既知の単一の値か、または単一の整数を指定します。

次の点に注意してください。

- 同じルール内の複数の s7commplus キーワードは、AND 演算されます。
- 同じルールで複数の s7commplus_func キーワードまたは s7commplus_opcode キーワードを使用すると、ルールが無効になります。無効にされたルールはトラフィックを照合できません。これらのキーワードで複数の値を検索するには、複数のルールを作成します。

s7commplus_content

s7commplus_content キーワードを使用して、検出カーソルを S7CommPlus パケットペイロードの先頭に配置します。S7CommPlus 侵入ルールで content または protected_content キーワードを使用する前に、このキーワードを設定することをお勧めします。

シンタックス：`s7commplus_content;`

例：`s7commplus_content;`

s7commplus_func

s7commplus_func キーワードを使用して、指定した S7CommPlus ヘッダーパラメータの 1 つと照合します。S7CommPlus パラメータ名または対応する 16 進コードを指定できます。

型：文字列

Syntax: `s7commplus_func: <header_parameter>;`

有効な値は、次のとおりです。

名前	コード
explore	0x04BB
createobject	0x04CA
deleteobject	0x04D4
setvariable	0x04F2
getlink	0x0524
setmultivar	0x0542
getmultivar	0x054C
beginsequence	0x0556
endsequence	0x0560
invoke	0x056B
getvarsubstr	0x0586
0x0 〜 0xFF	数式では追加の値を使用できることに注意してください。

例：`s7commplus_func: createobject;`

s7commplus_opcode

`s7commplus_opcode` キーワードを使用して、指定された S7CommPlus ヘッダーパラメータの 1 つと照合します。S7CommPlus パラメータ名または対応する 16 進コードを指定できます。

型：文字列

シンタックス：`s7commplus_opcode: <header_parameter>`

有効な値は、次のとおりです。

名前	コード
request	0x31
response	0x32
Notification	0x33
response2	0x02

名前	コード
0x0 〜 0xFF	数式では追加の値を使用できることに注意してください。

例：`s7commplus_opcode: 0x31;`

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。