S7CommPlus Inspector

S7CommPlus Inspector Overview

Type	Inspector (service)
Usage	Inspect
Instance Type	Multiton
Other Inspectors Required	`stream_tcp`
Enabled	`false`

S7CommPlus is a proprietary protocol developed by Siemens. S7CommPlus enables communication between programmable logic controllers of the Siemens S7 family of products.

The `s7commplus` inspector detects and analyzes S7CommPlus traffic. You can set intrusion rule options to alert on the specified S7CommPlus function and operation code header fields, and detect attacks in S7CommPlus traffic.

Best Practices for Configuring the S7CommPlus Inspector

If your network does not contain an enabled S7CommPlus device, you should not enable the `s7commplus` inspector in a network analysis policy that you apply to traffic.

S7CommPlus Inspector Parameters

S7CommPlus TCP port configuration

The `binder` inspector defines the S7CommPlus TCP port configuration. For more information, see the Binder Inspector Overview.

Example:

```
[
    {
        "when": {
            "role": "server",
            "proto": "tcp",
            "ports": "102"
        },
        "use": {
            "type": "s7commplus"
        }
    },
    {
        "when": {
            "role": "any",
            "service": "s7commplus"
        },
        "use": {
            "type": "s7commplus"
        }
    }
]
```

Note The `s7commplus` inspector does not provide any parameters.

S7CommPlus Inspector Rules

Enable the `s7commplus` inspector rules to generate events and, in an inline deployment, drop offending packets.

Table 1: S7CommPlus Inspector Rules

GID:SID	Rule Message
149:1	length in S7commplus MBAP header does not match the length needed for the given S7commplus function
149:2	S7commplus protocol ID is non-zero
149:3	reserved S7commplus function code in use

S7CommPlus Inspector Intrusion Rule Options

You can use the `s7commplus` keywords alone or in combination to create custom intrusion rules that identify attacks against traffic detected by the `s7commplus` inspector. For configurable keywords, specify a single known value or a single integer within the allowed range.

Note the following:

- Multiple `s7commplus` keywords in the same rule are AND-ed.
- Using multiple `s7commplus_func` or `s7commplus_opcode` keywords in the same rule negates the rule. The negated rule cannot match traffic. To search for multiple values with these keywords, create multiple rules.

s7commplus_content

Use the `s7commplus_content` keyword to position the detection cursor to the beginning of the S7CommPlus packet payload. We recommend that you set this keyword before you use a `content` or `protected_content` keyword in an S7CommPlus intrusion rule.

Syntax: `s7commplus_content;`

Examples: `s7commplus_content;`

s7commplus_func

Use the `s7commplus_func` keyword to match against one of the specified S7CommPlus header parameters. You can specify the S7CommPlus parameter name or the corresponding hexadecimal code.

Type: string

Syntax: `s7commplus_func: <header_parameter>;`

Valid values:

Name	Code
explore	0x04BB
createobject	0x04CA
deleteobject	0x04D4
setvariable	0x04F2
getlink	0x0524
setmultivar	0x0542
getmultivar	0x054C
beginsequence	0x0556
endsequence	0x0560
invoke	0x056B

Name	Code
`getvarsubstr`	`0x0586`
`0x0` through `0xFF`	Note that numeric expressions allow for additional values.

Examples: `s7commplus_func: createobject;`

s7commplus_opcode

Use the `s7commplus_opcode` keyword to match against one of the specified S7CommPlus header parameters. You can specify the S7CommPlus parameter name or the corresponding hexadecimal code.

Type: string

Syntax: `s7commplus_opcode: <header_parameter>`

Valid values:

Name	Code
`request`	`0x31`
`response`	`0x32`
`notification`	`0x33`
`response2`	`0x02`
`0x0` through `0xFF`	Note that numeric expressions allow for additional values.

Examples: `s7commplus_opcode: 0x31;`