MMS Inspector

MMS Inspector Overview

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

IEC 61850 is an international standard that defines communication protocols for electric power systems. The Manufacturing Message Specification (MMS) protocol is one of the IEC 61850 protocols. MMS enables the real-time transfer of Supervisory Control and Data Acquisition (SCADA) data between various manufacturing and process control devices. The MMS protocol uses TCP port 102 to exchange messages between client and server devices.

The `mms` inspector detects and analyzes MMS traffic. MMS messages may include multiple Protocol Data Units (PDUs) within one TCP packet, one PDU split across multiple TCP packets, or a combination of the two message configurations. The `mms` inspector normalizes the MMS traffic to present complete MMS messages to a device.

You write Snort 3 rules for MMS messages without decoding the MMS protocol. The `mms` inspector analyzes the OSI layers that encapsulate the MMS protocol, and provides access to certain MMS protocol fields and data content through rule options. For information about the MMS rule options, see MMS Inspector Intrusion Rule Options, on page 2

MMS Inspector Parameters

MMS service configuration

The binder inspector defines the MMS service configuration. For more information, see the Binder Inspector Overview.

Example:

```
[
    {
        "when": {
            "service": "mms"
        },
        "use": {
            "type": "mms"
        }
    }
]
```

MMS Inspector Rules

The mms inspector does not have any associated rules.

MMS Inspector Intrusion Rule Options

mms_data

Sets the detection cursor position to the start of the MMS Protocol Data Unit (PDU), bypassing all of the OSI encapsulation layers. When an intrusion rule includes mms_data, the next rule options in the rule begin processing from the MMS PDU.

Syntax: mms_data;

Examples:

The following sample intrusion rule sets the mms_data rule option. The mms_data rule option positions the detection cursor to the start of the MMS PDU, and checks the byte at that position for the value of an Initiate-Request message.

```
alert tcp ( \
msg: "PROTOCOL-SCADA MMS Initiate-Request"; \
flow: to_server, established; \
mms_data; \
content:"|A8|", depth 1; \
sid:1000000; \
)
```

mms_func

Compares the provided function name or number with the Confirmed Service field in the MMS request or response. Alert when the MMS function name or number matches the Confirmed Service.

Type: `string`

Syntax: `mms_func <function>;`

Examples:

The following sample intrusion rule sets the `mms_func` rule option and alerts when the `Confirmed Service Request` service matches the provided function name. In addition, `mms_func` enables the fast pattern matching feature to match on the `Confirmed Service Request (0xA0)` message.

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

The following sample intrusion rule sets the `mms_func` rule option and alerts when the `GetNameList` message matches the function number.

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