Talos Vulnerability Report

TALOS-2021-1236

MZ Automation GmbH lib60870.NET ASDU message processing denial of service vulnerability

APRIL 26, 2021

CVE NUMBER

CVE-2021-21778

Summary

A denial of service vulnerability exists in the ASDU message processing functionality of MZ Automation GmbH lib60870.NET 2.2.0. A specially crafted network request can lead to loss of communications. An attacker can send an unauthenticated message to trigger this vulnerability.

Tested Versions

MZ Automation GmbH lib60870.NET 2.2.0

Product URLs

https://github.com/mz-automation/lib60870.NET

CVSSv3 Score

7.5 - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

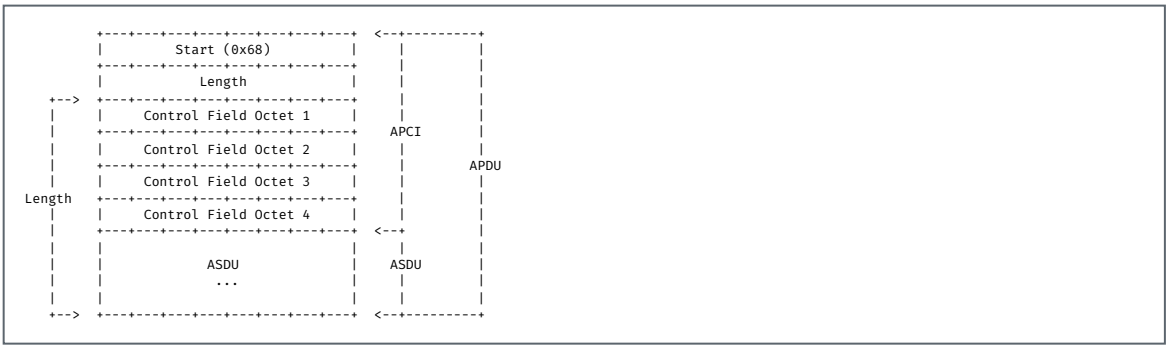
CWE

CWE-617 - Reachable Assertion

Details

lib60870.NET is a .NET implementation of the IEC60870 protocol specification. This library can be used as a building block to implement communications defined within IEC60870 into a custom client/server application.

Contained within the lib60870.NET is an implementation of the IEC60870-5-104 (hereafter IEC104) protocol. IEC104 is a protocol used to transmit simple control messages between the central station and various outstations. It consists of a few information groupings: APDU, APCI, and (conditionally) ASDU. All message types contain the APDU and APCI while only Information Transfer control type messages (hereafter Type I) contain an ASDU. The layout of these message groups is similar to the following (ref: 60870-5-104 specification):



When an IEC104 Type I message is sent, the specification requires a length of at least (but often more than) nine bytes.

lib60870.NET performs a check to verify that a message of the proper size is being processed, however if the check fails an ASDUParsingException is triggered, causing the application to exit and stopping all communication until an application restart is performed.

The problematic code can be found in lib60870/CS101/ASDU.cs, a snippet of which is shown below:

```
public ASDU(ApplicationLayerParameters parameters, byte[] msg, int bufPos, int msgLength)
{
    this.parameters = parameters;

    int asduHeaderSize = 2 + parameters.SizeOfCOT + parameters.SizeOfCA;

    // vulnerable code
    if ((msgLength - bufPos) < asduHeaderSize)
        throw new ASDUParsingException("Message header too small");

    typeId = (TypeID)msg[bufPos++];

    ...
```

An example implementation of this code can be found in the IEC 60870-5-104 Test Tool application (IEC60870TestMaster.exe) which can be obtained from MZ Automation.

Crash Information

```
An unhandled exception occurred in IEC60870TestMaster.exe
Exception: lib60870.ASDUParsingException
Message: Message header too small
```

Timeline

2021-02-04 - Vendor Disclosure

2021-04-26 - Public Release

CREDIT

Discovered by Jared Rittle of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT TALOS-2020-1142

NEXT REPORT TALOS-2021-1361