

# Report

## Cybersecurity Advisory for M-Bus

Attachments

## Contents

|                                 |          |
|---------------------------------|----------|
| <b>1 Overview</b>               | <b>2</b> |
| <b>2 Affected Versions</b>      | <b>2</b> |
| <b>3 Vulnerability Details</b>  | <b>2</b> |
| 3.1 CVE-2026-76815 . . . . .    | 2        |
| <b>4 Mitigation Steps</b>       | <b>3</b> |
| <b>5 Acknowledgements</b>       | <b>3</b> |
| <b>6 Additional Information</b> | <b>3</b> |

## 1 Overview

This advisory addresses a cybersecurity vulnerability discovered in the M-Bus Modbus library. The vulnerability may allow denial of service and data integrity compromise, and requires immediate action to mitigate potential exploitation.

M-Bus devices located on networks that are isolated from potential attackers, such as internal networks or those protected by firewalls, have reduced exposure to the identified threat.

## 2 Affected Versions

- M-Bus versions prior to 1.0.1

## 3 Vulnerability Details

### 3.1 CVE-2026-76815

|                             |                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE ID</b>               | CVE-2026-76815                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>          | Out-of-bounds write in mbus_read()                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Impact</b>               | Denial of service, Data integrity                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Exploitability</b>       | This vulnerability can be exploited by a malicious or man-in-the-middle Modbus slave capable of sending crafted responses to a Modbus master using the M-Bus library. The attacker-controlled length and data, combined with typical stack-allocated buffers, creates an exploitable memory corruption primitive. The vulnerability requires no authentication as the Modbus protocol provides none. |
| <b>CVSS v3.1 Base Score</b> | 7.5                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>CVSS v3.1 Vector</b>     | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H                                                                                                                                                                                                                                                                                                                                                         |
| <b>CWE</b>                  | CWE-130: Improper Handling of Length<br>Parameter Inconsistency<br>CWE-120: Buffer Copy without Checking Size of Input                                                                                                                                                                                                                                                                               |

---

|                       |                                |
|-----------------------|--------------------------------|
| <b>Recommendation</b> | Upgrade to M-Bus version 1.0.1 |
|-----------------------|--------------------------------|

---

## 4 Mitigation Steps

Affected users are advised to upgrade to M-Bus version 1.0.1 to mitigate the identified vulnerability.

As an alternative measure and to enhance security, ensure that M-Bus devices are not connected to untrusted networks. Devices that are not accessible to potential attackers, such as those on isolated networks or protected by firewalls, have reduced exposure to potential threats.

## 5 Acknowledgements

We acknowledge the efforts of f0rw4rd from quellsec.dev who identified and reported this vulnerability.

## 6 Additional Information

For further inquiries or support, please contact:

- **Support Contact:** [support@rt-labs.com](mailto:support@rt-labs.com)
- **Website:** <https://www.rt-labs.com>
- **Security Information:** <https://rt-labs.com/cyber-security/>

**Disclaimer:** This advisory is provided for informational purposes only. RT-Labs is not liable for any damage caused by the exploitation of the vulnerability listed.