Denial-of-Service (DoS) Vulnerability due to OpenSSL Vulnerability in MELSOFT MaiLab

Release date: July 18, 2024
Mitsubishi Electric Corporation

Overview

Denial-of-Service (DoS) vulnerability due to OpenSSL vulnerability exists in MELSOFT MaiLab. An attacker may be able to cause a denial-of-service (DoS) condition in the target product by sending a specially crafted message authentication code. (CVE-2023-4807)

CVSS[1]

CVE-2023-4807 CVSS:v3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score: 5.9

Affected products

The affected products are as follows:

No	Product name	Model name	Affected software versions
1	MELSOFT MaiLab	SW1DND-MAILAB-M SW1DND-MAILABPR-M	ver.1.00A to 1.05F

【How to check the version】

(1) Launch MELSOFT MaiLab.
(2) Check the version information displayed in the opened “Configure Tool” (refer to Figure 1).

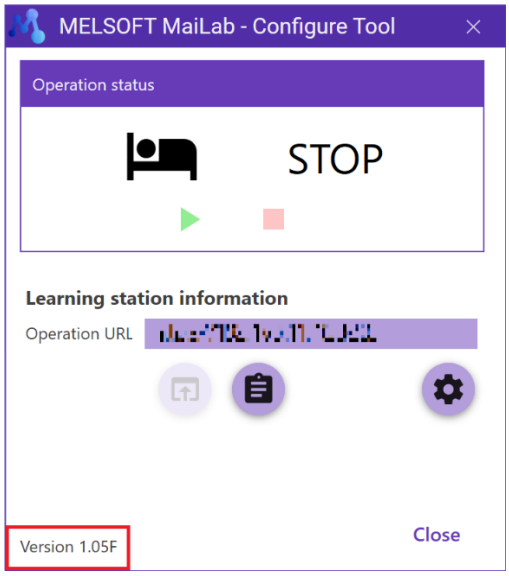

Figure1 MELSOFT MaiLab Screen

Description

A denial of service vulnerability exists in the OpenSSL library used in MELSOFT MaiLab due to improper verification of cryptographic signature (CWE-347[2]) resulting from improper implementation of the POLY1305 Message Authentication Code (MAC).

Impact

An attacker could cause a denial-of-service (DoS) condition in the affected product by selecting a mode that uses POLY1305 authenticated encryption during TLS communication and sending a specially crafted message authentication code.

Countermeasures

Please install the fixed version listed in the table below and update your software.
For information about how to install the fixed version, please contact your local Mitsubishi Electric representative.

No	Product name	Model name	Fixed software versions
1	MELSOFT MaiLab	SW1DND-MAILAB-M SW1DND-MAILABPR-M	ver.1.06G or later

[1] https://www.first.org/cvss/v3.1/specification-document

[2] https://cwe.mitre.org/data/definitions/347.html

Mitigations / Workarounds

Mitsubishi Electric recommends that customers take the following mitigations to minimize the risk of exploiting this vulnerability:

- When internet access is required, use a firewall or a Virtual Private Network (VPN) to prevent unauthorized access.
- Use the products within a control system, and protect the network and devices in the control system with a firewall to block access from untrusted networks and hosts.
- Restrict physical access to the PC on which the product is installed and the network to which the PC is connected to prevent unauthorized access.
- Do not click on web links in emails or other messages from untrusted sources. Also, do not open attachments from untrusted emails.

Contact information

Please contact your local Mitsubishi Electric representative.

< Inquiries | MITSUBISHI ELECTRIC FA >
https://www.mitsubishielectric.com/fa/support/index.html