Arbitrary code execution vulnerability in MELSOFT FieldDeviceConfigurator product

Release date: February 16, 2021
Last update date: June 17, 2021
Mitsubishi Electric Corporation

■Overview

MELSOFT FieldDeviceConfigurator provided by Mitsubishi Electric contains a vulnerability caused by fdtCONTAINER component manufactured by M&M Software. A malicious attacker could use this vulnerability to obtain information, corrupt information, tamper information, cause a denial-of-service (DoS), and so on. (CVE-2020-12525)
The version of MELSOFT FieldDeviceConfigurator affected by this vulnerability is shown below. Please implement the countermeasures or mitigations described below.

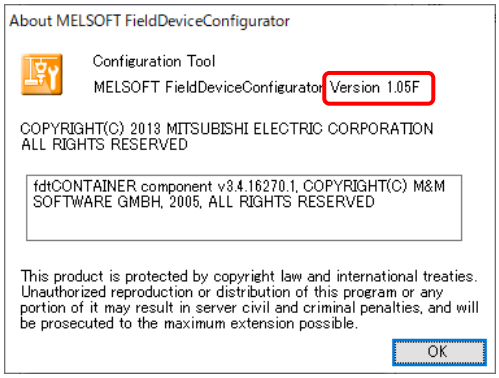
■CVSS

CVE-2020-12525　CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H　Base Score:7.3

■Affected products

The affected product and versions are:
- MELSOFT FieldDeviceConfigurator, versions 1.05F and prior

<How to Check the Version>
1. Run the product.
2. Click [Help]-> [About] in the menu.
3. The [About MELSOFT FieldDeviceConfigurator] screen is displayed. Check the version.



■Description

MELSOFT FieldDeviceConfigurator provided by Mitsubishi Electric contains the vulnerability CVE-2020-12525 in which malicious code is executed due to the CWE-502: Deserialization of Untrusted Data in the fdtCONTAINER component manufactured by M&M Software.

■Impact

When a customer opens a project with malicious code embedded by an attacker, the malicious code could be executed with user privileges, resulting in information disclosure, information corruption, information tampering, denial-of-service (DoS), and so on.

■Countermeasures

Please download version 1.06G or later from the following site and update it:
https://www.mitsubishielectric.com/fa/#software

<How to Update the product>
1. Uninstall the old version.
2. Unzip the downloaded file (zip format).
3. Double-click the file "setup.exe" located in the folder unzipped and install it.

■Mitigations

Mitsubishi Electric recommends that customers take the following mitigations to minimize the risk of exploiting this vulnerability:
- Make sure that a file obtained from trusted person by trusted route, when you obtain the DTM configuration file (*.dtmx) used in MELSOFT FieldDeviceConfigurator.
- Operate the product with an account that does not have administrator's privileges.

- Install an antivirus software in your personal computer.

■Contact information

Please contact your local Mitsubishi Electric representative.

< Inquiries | MITSUBISHI ELECTRIC FA >

https://www.mitsubishielectric.com/fa/support/index.html

■Update history

June 17, 2021

Added MELSOFT FieldDeviceConfigurator that has been fixed to “Affected products” and “Countermeasures”.