Arbitrary Code Execution Vulnerabilities due to 7-Zip Vulnerability in MELSOFT Update Manager

Release date: July 3, 2025
Mitsubishi Electric Corporation

Overview

Arbitrary code execution vulnerabilities due to Integer Underflow (Wrap or Wraparound) (CWE-191[1]) and Protection Mechanism Failure (CWE-693[2]) exist in 7-Zip, the file compression/decompression software included in MELSOFT Update Manager. An attacker may execute arbitrary malicious code by getting 7-Zip, which is included in MELSOFT Update Manager, to decompress a specially crafted compressed file. As a result, the attacker may disclose, tamper with information, or cause a denial-of-service (DoS) condition on the product.

The affected versions of MELSOFT Update Manager are listed below, so please take countermeasures described in “Countermeasures for Customers” section.

CVSS[3]

CVE-2024-11477	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H Base Score: 8.1
CVE-2025-0411	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H Base Score: 7.8

Affected products

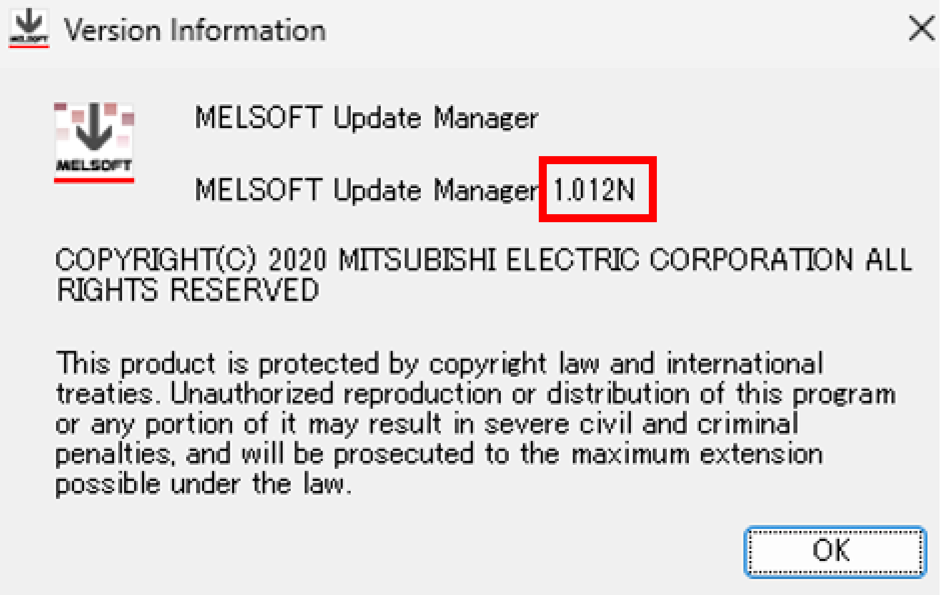
The affected products and versions are below.

Product	Model Number	Version
MELSOFT Update Manager (Note)	SW1DND-UDM-M	1.000A～1.012N

(Note) MELSOFT Update Manager is a product that is only available through your local Mitsubishi Electric representative outside of Japan.

How to Check the Version Number in Use:

1. Launch MELSOFT Update Manager and select "Version Information of MELSOFT Update Manager" from the "Menu".
2. The version number of the running MELSOFT Update Manager will be displayed in the area surrounded by a red-frame in the window (refer to Figure 1).



Version Information

MELSOFT Update Manager

MELSOFT Update Manager 1.012N

COPYRIGHT(C) 2020 MITSUBISHI ELECTRIC CORPORATION ALL RIGHTS RESERVED

This product is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program or any portion of it may result in severe civil and criminal penalties, and will be prosecuted to the maximum extension possible under the law.

Figure 1. MELSOFT Update Manager Version Information Screen

[1] https://cwe.mitre.org/data/definitions/191.html

[2] https://cwe.mitre.org/data/definitions/693.html

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

Description

Multiple vulnerabilities below exist in the file compression/decompression software 7-Zip included in MELSOFT Update Manager.

CVE ID	Description of the Vulnerability
CVE-2024-11477	Remoet Code Execution Vulnerability due to Integer Underflow (Wrap or Wraparound) (CWE-191).
CVE-2025-0411	Malicious Code Execution Vulnerability due to Protection Mechanism Failure (CWE-693).

Impact

An attacker may execute arbitrary malicious code by getting 7-Zip, which is included in MELSOFT Update Manager, to decompress a specially crafted compressed file. As a result, the attacker may disclose, tamper with information, or cause a denial-of-service (DoS) condition on the product.

Countermeasures for Customers

[For customers in Japan]

Please download version 1.013P or later from the download site below, and follow the update procedure below (Note). Additionally, please verify the authenticity of the following download site in advance.

<Download Site (in Japanese)>

https://www.mitsubishielectric.co.jp/fa/download/index.html

<Update Procedure>

1. Extract the downloaded file (in zip format).
2. Run "setup.exe" in the extracted folder to install.

(Note) If you are using MELSOFT Update Manager version 1.012N and prior, please do not connect to the internet until the above update is complete. There is a risk that these vulnerabilities could be exploited.

[For customers outside Japan]

For information about how to install the fixed version, please contact your local Mitsubishi Electric representative.

Mitigations / Workarounds

For customers who cannot immediately update the product, Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting these vulnerabilities.

(1) Use the PC with the affected product within the LAN and block remote logins from untrusted networks, hosts, and users.

(2) When connecting the PC with the affected product to the internet, use a firewall, virtual private network (VPN), etc. to prevent unauthorized access and allow only trusted users to remote login.

(3) Restrict physical access to the PC with the affected product and the network to which the PC is connected to, to prevent unauthorized physical access .

(4) Do not click on web links in emails from untrusted sources. Also, do not open attachments in untrusted emails.

(5) Install antivirus software on the PC with the affected product.

Contact information

Please contact your local Mitsubishi Electric representative.

< Inquiries | Mitsubishi Electric FA >

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