Multiple Vulnerabilities in the 7-Zip component included in MELSOFT Update Manager

Release date: June 30, 2026
Mitsubishi Electric Corporation

Overview

Denial-of-service (DoS) vulnerabilities due to Heap-based Buffer Overflow (CWE-122[1]) and NULL Pointer Dereference (CWE-476[2]), an information tampering vulnerability due to Improper Link Resolution Before File Access ('Link Following') (CWE-59[3]) , and a malicious code execution vulnerability due to Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (CWE-22[4]) exist in the 7-Zip component, the file compression/decompression software included in MELSOFT Update Manager. An attacker may be able to trigger a buffer overflow or a NULL pointer dereference that may cause the affected product to enter a denial-of-service (DoS) condition by getting a legitimate user to decompress a specially crafted archive file using the 7-Zip component included in MELSOFT Update Manager (CVE-2025-53816, CVE-2025-53817). An attacker may also be able to tamper with or destroy information by using the similar method (CVE-2025-55188). If tampered or destroyed files are required for PC operation, the affected PC may enter a denial-of-service (DoS) condition. Furthermore, an attacker may be able to execute a malicious code by decompressing a specially crafted archive file using the 7-Zip component included in MELSOFT Update Manager (CVE-2025-11001). As a result of the execution of a malicious program, the affected product may be impacted in ways such as information theft, information tampering, a denial-of-service (DoS) condition, or other impacts.

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

CVSS[5]

CVE-2025-53816 CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N Base Score:5.1
CVE-2025-53817 CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N Base Score:5.1
CVE-2025-55188 CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:P/VC:N/VI:H/VA:N/SC:N/SI:H/SA:H Base Score:6.9
CVE-2025-11001 CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H Base Score:9.3

Affected products

The affected products and versions are listed below.

Product	Model Number	Version
MELSOFT Update Manager (Note)	SW1DND-UDM-M	1.000A to 1.014Q

(Note) MELSOFT Update Manager is available only through your local Mitsubishi Electric representative for customers outside of Japan.

How to Check the Version Number in Use:

1. Start 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 outlined in red in the window (Refer to Figure 1).

[1] https://cwe.mitre.org/data/definitions/122.html
[2] https://cwe.mitre.org/data/definitions/476.html
[3] https://cwe.mitre.org/data/definitions/59.html
[4] https://cwe.mitre.org/data/definitions/22.html
[5] https://www.first.org/cvss/v4-0/specification-document

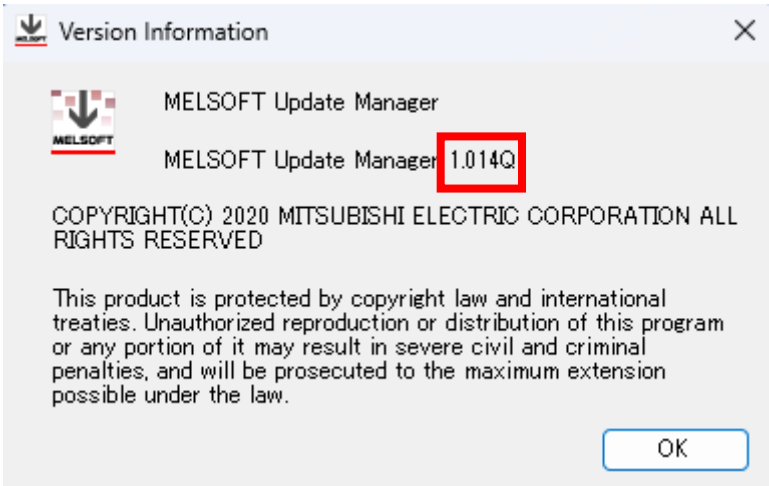

Figure 1. MELSOFT Update Manager Version Information Screen

Description

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

CVE ID	Description of the Vulnerability
CVE-2025-53816	Denial-of-service (DoS) vulnerability due to Heap-based Buffer Overflow. (CWE-122)
CVE-2025-53817	Denial-of-service (DoS) vulnerability due to NULL Pointer Dereference. (CWE-476)
CVE-2025-55188	Information tampering vulnerability due to Improper Link Resolution Before File Access ('Link Following'). (CWE-59)
CVE-2025-11001	Malicious code execution vulnerability due to Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'). (CWE-22)

Impact

CVE-2025-53816:
An attacker may be able to trigger a buffer overflow that may cause the affected product to enter a denial-of-service (DoS) condition by getting a legitimate user to decompress a specially crafted archive file using the 7-Zip component included in MELSOFT Update Manager.

CVE-2025-53817:
An attacker may be able to trigger a NULL pointer dereference that may cause the affected product to enter a denial-of-service (DoS) condition by getting a legitimate user to decompress a specially crafted archive file using the 7-Zip component included in MELSOFT Update Manager.

CVE-2025-55188:
An attacker may be able to tamper with or destroy information by getting a legitimate user to decompress a specially crafted archive file using the 7-Zip component included in MELSOFT Update Manager. If tampered or destroyed files are required for PC operation, the affected PC may enter a denial-of-service (DoS) condition.

CVE-2025-11001:
An attacker may be able to execute a malicious code by decompressing a specially crafted archive file using the 7-Zip component included in MELSOFT Update Manager. As a result, the attacker may thieve information, tamper with information, cause a denial-of-service (DoS) condition in the product, or cause other impacts.

Countermeasures for Customers

[For customers in Japan]
Please download version 1.015R or later from the download site below, and follow the update procedure below.
<Download Site (in Japanese)>
https://www.mitsubishielectric.co.jp/fa/download/index.html

<Update Procedure>
1. Decompress the downloaded file (in zip format).
2. Run "setup.exe" in the extracted folder to install.

[For customers outside Japan]
For information about how to install the fixed version, please contact your local Mitsubishi Electric representative.

Countermeasures for Products

The fixed versions are listed below.

Product	Model Number	Version
MELSOFT Update Manager (Note)	SW1DND-UDM-M	1.015R or later

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/service-support/index.html