MELSOFT Update Manager に搭載の 7-Zip における 複数の悪意のあるプログラムが実行される脆弱性

公開日 2025 年 7 月 3 日
最終更新日 2025 年 12 月 16 日
三菱電機株式会社

■概要

MELSOFT Update Manager に搭載しているファイル圧縮・解凍用ソフトウェア 7-Zip において、整数アンダーフロー(CWE-191[1])及び保護メカニズムの不具合(CWE-693[2])に起因する複数の悪意のあるプログラムが実行される脆弱性が存在することが判明しました。攻撃者は、MELSOFT Update Manager に搭載している 7-Zip で、細工した圧縮ファイルを正規ユーザに解凍させることによって、悪意のあるプログラムを実行できる可能性があります。結果として、情報を窃取される、情報を改ざんされる、サービス停止(DoS)状態にされる等の影響を受ける可能性があります。

これらの脆弱性の影響を受ける MELSOFT Update Manager のバージョンを以下に示しますので、対策方法に記載の内容を実施してください。

■CVSS スコア [3]

CVE-2024-11477　CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H 基本値:8.2
CVE-2025-0411　CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H 基本値:7.5

■該当製品の確認方法

影響を受ける製品は以下の通りです。

製品	形名	バージョン
MELSOFT Update Manager	SW1DND-UDM-M	1.000A～1.012N

使用しているバージョン番号の確認方法は以下の通りです。

1. MELSOFT Update Manager を起動し、「メニュー」から「MELSOFT Update Manager のバージョン情報」を選択します。
2. 表示されるウィンドウの赤枠部分が、起動している MELSOFT Update Manager のバージョン番号です。(図 1 参照)

図 1.MELSOFT Update Manager バージョン情報画面

■脆弱性の説明

MELSOFT Update Manager に搭載しているファイル圧縮・解凍用ソフトウェア 7-Zip には、以下の 2 件の脆弱性が存在します。

CVE ID	脆弱性の説明
CVE-2024-11477	整数アンダーフロー(CWE-191)による悪意のあるプログラムが実行される脆弱性
CVE-2025-0411	保護メカニズムの不具合(CWE-693)による悪意のあるプログラムが実行される脆弱性

1 https://cwe.mitre.org/data/definitions/191.html
2 https://cwe.mitre.org/data/definitions/693.html
3 https://www.ipa.go.jp/security/vuln/CVSSv3.html

■脆弱性がもたらす脅威

攻撃者は、MELSOFT Update Manager に搭載している 7-Zip で、細工した圧縮ファイルを正規ユーザに解凍させることによって、悪意のあるプログラムを実行できる可能性があります。結果として、情報を窃取される、情報を改ざんされる、サービス停止(DoS)状態にされる等の影響を受ける可能性があります。

■お客様での対応

下記ダウンロードサイトよりバージョン 1.013P 以降をダウンロードしたうえで、下記アップデート方法に従ってアップデートしてください。

〈ダウンロードサイト〉

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

〈アップデート方法〉

1. ダウンロードしたファイル(zip 形式)を解凍します。
2. 解凍されたフォルダの中の「setup.exe」を実行してインストールを行います。

■軽減策・回避策

すぐに製品をアップデートできないお客様に対して、これらの脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。

(1) 該当製品がインストールされた PC を LAN 内で使用し、信頼できないネットワークやホスト、ユーザからのリモートログインをブロックします。
(2) 該当製品がインストールされた PC をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等で不正アクセスを防止したうえで、信頼できるユーザのみにリモートログインを許可します。
(3) 該当製品がインストールされた PC および本 PC が接続されているネットワークへの物理的なアクセスを制限し、不正な接触を防止します。
(4) 信頼できない送信元からのメール等に記載された Web リンクをクリックしないようにします。また信頼できない電子メールの添付ファイルを開かないようにします。
(5) 当該製品を使用するパソコンにウイルス対策ソフトを搭載してください。

■お客様からのお問い合わせ先

製品をご購入いただいた弊社の支社、代理店にご相談ください。

〈お問い合わせ | 三菱電機 FA〉

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

■更新履歴

2025 年 12 月 16 日

・「CVSS スコア」を更新しました。
・ 上記に伴い、「件名」「概要」「脆弱性がもたらす脅威」及び「お客様での対応」を修正しました。