MELSOFT Update Manager に搭載の 7-Zip における複数の脆弱性

公開日 2026 年 6 月 30 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、ヒープベースのバッファオーバーフロー(CWE-122[1])及び NULL ポインタデリファレンス(CWE-476[2])によるサービス拒否(DoS)の脆弱性、リンク解釈の問題(CWE-59[3])による情報改ざんの脆弱性並びにパス・トラバーサル(CWE-22[4])による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り、バッファオーバーフローや NULL ポインタ参照を発生させ、対象をサービス停止(DoS)状態に陥らせることができる可能性があります(CVE-2025-53816、CVE-2025-53817)。また、攻撃者は、同様の手段により、情報を改ざん又は破壊できる可能性があります(CVE-2025-55188)。改ざん又は破壊されたファイルが PC の動作に必要なファイルの場合には、当該 PC がサービス停止(DoS)状態に陥る可能性があります。さらに、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解凍することにより、悪意のあるプログラムを実行できる可能性があります(CVE-2025-11001)。悪意のあるプログラムが実行される結果として、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、お客様での対応に記載の内容を実施してください。

■CVSS スコア [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	基本値: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	基本値: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	基本値: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	基本値:9.3

■該当製品の確認方法

影響を受ける製品は、以下のとおりです。

製品	形名	バージョン
MELSOFT Update Manager	SW1DND-UDM-M	1.000A～1.014Q

使用しているバージョン番号の確認方法は、以下のとおりです。

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

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

■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 4 件の脆弱性が存在します。

CVE ID	脆弱性の説明
CVE-2025-53816	ヒープベースのバッファオーバーフロー(CWE-122)によるサービス拒否(DoS)の脆弱性
CVE-2025-53817	NULL ポインタデリファレンス(CWE-476)によるサービス拒否(DoS)の脆弱性
CVE-2025-55188	リンク解釈の問題(CWE-59)による情報改ざんの脆弱性
CVE-2025-11001	パス・トラバーサル(CWE-22)による悪意のあるプログラムが実行される脆弱性

■脆弱性がもたらす脅威

CVE-2025-53816:

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り、ヒープベースのバッファオーバーフローを発生させ、対象をサービス停止(DoS)状態に陥らせることができる可能性があります。

CVE-2025-53817:

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り、NULL ポインタ参照を発生させ、対象をサービス停止(DoS)状態に陥らせることができる可能性があります。

CVE-2025-55188:

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り、ファイルを改ざんしたり、破壊することができる可能性があります。改ざん又は破壊されたファイルが PC の動作に必要なファイルの場合には、当該 PC がサービス停止(DoS)状態に陥る可能性があります。

CVE-2025-11001:

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解凍することにより、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、情報を取得される、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 1.015R 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。

■製品での対応

対策済みのバージョンは以下のとおりです。

製品	形名	バージョン
MELSOFT Update Manager	SW1DND-UDM-M	1.015R 以降

■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/purchase/index.html