MELIPC シリーズ MI5122-VW における
悪意のあるプログラムが実行される脆弱性

公開日 2024 年 7 月 4 日
三菱電機株式会社

■概要
MELIPC シリーズ MI5122-VW にプリインストールされているスマートデバイス通信ゲートウェイには、不適切なデフォルトパーミッション(CWE-276[1])により、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。ローカルログインした攻撃者が、特定のフォルダに悪意のあるプログラムを保存することによって、対象製品に悪意のあるプログラムを実行させることができます。その結果、情報を窃取される、情報を改ざん・破壊・削除される、サービス停止(DoS)状態にされるなどの可能性があります。(CVE-2024-3904)
この脆弱性の影響を受ける製品型名およびバージョンを以下に示します。

■CVSS スコア [2]
CVE-2024-3904　CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H　基本値:8.8

■該当製品の確認方法
影響を受ける製品は以下の製品です。

シリーズ	型名	バージョン
MELIPC シリーズ	MI5122-VW	ファームウェアバージョン"05"～"07"

ファームウェアバージョンの確認方法は、以下のマニュアルを参照ください。
・MELIPC MI5000 シリーズ ユーザーズマニュアル(スタートアップ編)「付 17 製造情報・ファームウェアバージョン」

各種製品マニュアルは以下サイトよりダウンロードが可能です。
https://www.mitsubishielectric.co.jp/fa/download/index.html

■脆弱性の説明
MELIPC シリーズ MI5122-VW にプリインストールされているスマートデバイス通信ゲートウェイには、不適切なデフォルトパーミッション(CWE-276)により、悪意のあるプログラムが実行される脆弱性が存在します。

■脆弱性がもたらす脅威
ローカルログインした攻撃者が、特定のフォルダに悪意のあるプログラムを保存することによって、対象製品に悪意のあるプログラムを実行させることができます。その結果、情報を窃取される、情報を改ざん・破壊・削除される、サービス停止(DoS)状態にされるなどの可能性があります。

■対策方法
<MELIPC シリーズの該当製品をご使用中のお客様>
該当製品・該当バージョンをご使用のお客様は、回避策および軽減策にて対応ください。
次項の通り対策済み製品をリリースしておりますが、対策版へのアップデートは出来ません。

■製品での対応
下記の製品において、不適切なデフォルトパーミッションを設定しないよう対策済です。

シリーズ	型名	バージョン
MELIPC シリーズ	MI5122-VW	ファームウェアバージョン"08"以降

1 https://cwe.mitre.org/data/definitions/276.html
2 https://www.ipa.go.jp/security/vuln/CVSSv3.html

■回避策

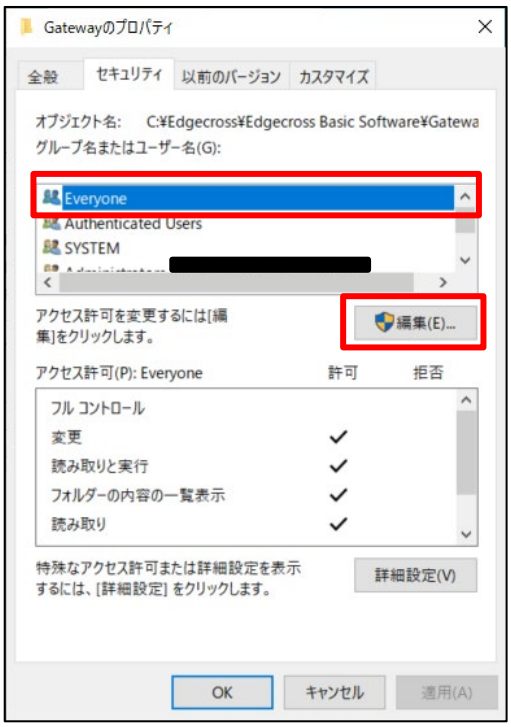
以下の手順にて対象フォルダのアクセス権限をご確認いただき、Everyone に対するアクセス権限の削除をお願いします。

[対象フォルダ]

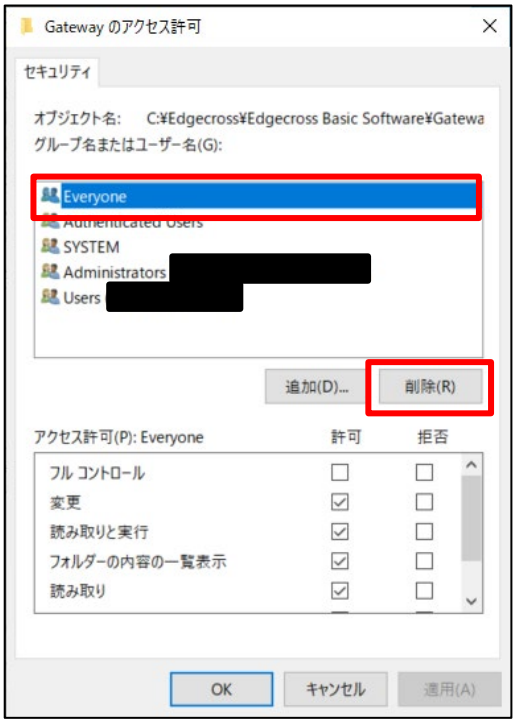
C:¥Edgecross¥Edgecross Basic Software¥Gateway¥
C:¥Edgecross¥Edgecross Basic Software¥Gateway¥ITGWMDA_000002_SDCommGateway¥
C:¥Edgecross¥Edgecross Basic Software¥Gateway¥ITGWMDA_000002_SDCommGateway¥settings
C:¥Edgecross¥Edgecross Basic Software¥Gateway¥ITGWMDA_000002_SDCommGateway¥icon
C:¥Edgecross¥Edgecross Basic Software¥Gateway¥ja-JP¥
C:¥Edgecross¥Edgecross Basic Software¥Gateway¥zh-CN¥
C:¥Edgecross¥Edgecross Basic Software¥Gateway¥ITGWMDA_000002_SDCommGateway¥Doc

[手順]

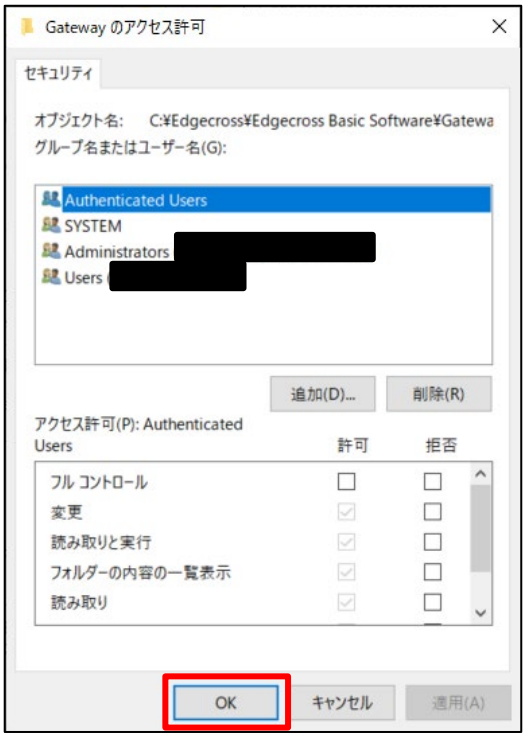
(1) 対象フォルダを右クリックし、プロパティを選択する
(2) セキュリティタブを選択し、Everyone が存在する場合は編集ボタンを押下する
(Everyone が存在しない場合は問題無いため、手順終了)



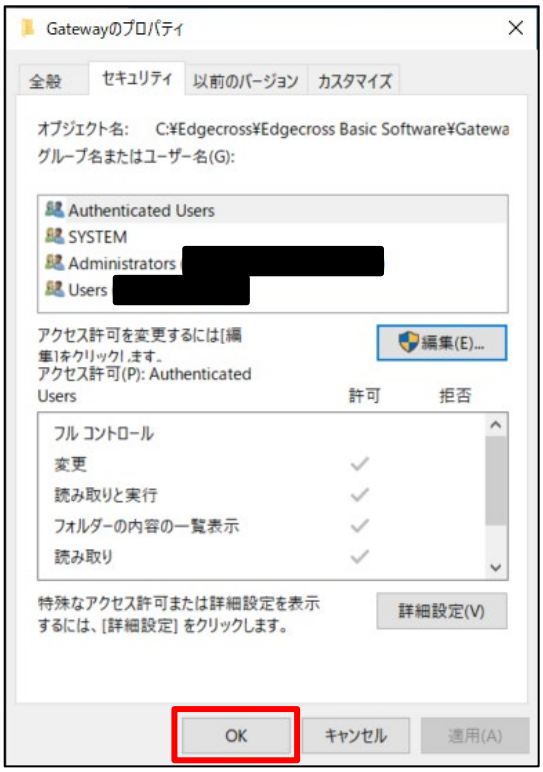
(3) Everyone を選択し、削除ボタンを押下する



(4)　OK ボタンを押下してアクセス許可画面を閉じる



(5)　OK ボタンを押下してプロパティ画面を閉じる



■軽減策

本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。

・該当製品にウイルス対策ソフトを搭載する。
・該当製品及び該当製品が接続された LAN への物理的なアクセスを制限する。
・該当製品を 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する。
・該当製品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する。
・信頼できないファイルを開いたり、信頼できないリンクをクリックしない。

■お客様からのお問い合わせ先
製品をご購入いただいた当社の支社、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