MELSEC WS シリーズ Ethernet インタフェースユニットにおける認証回避の脆弱性

公開日 2024 年 1 月 30 日
三菱電機株式会社

■概要
MELSEC WS シリーズ Ethernet インタフェースユニットに、認証回避の脆弱性が存在することが判明しました。権限のない攻撃者が、キャプチャリプレイ攻撃*1 により認証を回避して、当該ユニットに不正にログインすることができます。結果として、不正にログインした攻撃者は、ユニット内のプログラムやパラメータの閲覧及び改ざんを行える可能性があります。(CVE-2023-6374)

*1: 攻撃者が、正規のユーザがログインする時にネットワークを流れるログイン情報を、盗聴することにより取得し、取得したログイン情報を再送することで不正にログインを試行する攻撃

■CVSS スコア [1]
CVE-2023-6374 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N 基本値:5.9

■該当製品の確認方法
影響を受ける製品とシリアル番号は以下の通りです。

シリーズ	製品形名	シリアル番号
MELSEC WS シリーズ	WS0-GETH00200	全てのシリアル番号

■脆弱性の説明
MELSEC WS シリーズ Ethernet インタフェースユニットには、Capture-replay による認証回避(CWE-294[2])による認証回避の脆弱性が存在します。

■脆弱性がもたらす脅威
権限のない攻撃者が、キャプチャリプレイ攻撃により認証を回避して、当該ユニットに不正にログインすることができます。結果として、ユニット内のプログラムやパラメータの閲覧及び改ざんを行える可能性があります。

■対策方法
軽減策・回避策にて対応をお願いいたします。

■軽減策・回避策
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。
・当該製品と通信相手との間の通信を、仮想プライベートネットワーク(VPN)等を使用して暗号化してください。
・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)等を使用し、不正アクセスを防止してください。
・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からのアクセスをファイアウォールでブロックしてください。
・該当製品並びに該当製品が接続された LAN 内に配置されたパソコン及びネットワーク機器への物理的なアクセスを制限してください。

■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

1 https://www.ipa.go.jp/security/vuln/CVSSv3.html
2 https://cwe.mitre.org/data/definitions/294.html