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 2023 年 5 月 18 日
最終更新日 2023 年 8 月 22 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、Telnet で当該ユニットへ接続することにより、認証を回避して不正にログインすることができます。そのため、不正にログインした攻撃者は、ユニットをリセットすることが行え、さらに、特定の条件を満たした場合に、ユニットの設定内容の閲覧及び改ざん、並びにファームウェアの書き換えを行える可能性があります。(CVE-2023-1618)

■CVSS スコア [1]
CVE-2023-1618 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N 基本値:7.5

■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とおりです。

シリーズ	形名	シリアル番号
MELSEC WS シリーズ	WS0-GETH00200	シリアル番号の 2310 ****以前※1

※1 シリアル番号は、型式ラベルおよびオンライン状態の設定・モニタツールのハードウェア設定画面で確認できます。

■脆弱性の説明
該当製品は、工場出荷時の初期設定で非公開の Telnet 機能が有効となっており、権限のない攻撃者が Telnet で当該ユニットへ接続することにより、認証を回避して不正にログインすることができる脆弱性が存在します。(CWE-489)[2]

■脆弱性がもたらす脅威
権限のない攻撃者が Telnet でユニットに接続し、ユニットをリセットすることが行え、さらに、特定の条件を満たした場合に、ユニットの設定内容の閲覧及び改ざん、並びにファームウェアの書き換えを行える可能性があります。

■対策方法
以下のシリアル番号で対策済みです。

シリーズ	形名	シリアル番号
MELSEC WS シリーズ	WS0-GETH00200	シリアル番号の 2311 ****以降

該当製品をお持ちの場合は、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
Telnet のパスワードに、第三者に推測されにくいパスワードを設定してください。最大 15 文字のパスワードを設定することができます。
Telnet クライアントを使用し、以下の①～②を行うことにより、該当製品の Telnet のパスワードを変更できます。なお、入力文字列中の“␣“は半角の空白を表します。

① パスワードの設定
1) “telnet␣“と入力、続けて該当製品の IP アドレスを入力し Enter キーを押します。
2) “Password“と表示されたら、何も入力せず Enter キーを押します。
3) “telnet>“と表示されたら、“password␣“と入力、続けて設定したいパスワード文字列を入力後 Enter キーを押します。
4) 最後に“quit“と入力後 Enter キーを押します。

② パスワードが設定されていることを確認
1) ①を実施後に“telnet␣“と入力、続けて該当製品の IP アドレスを入力し Enter キーを押します。
2) “Password“と表示されたら、①で設定したパスワードを入力し、Enter キーを押します。
3) “telnet>“と表示されたら、パスワードは正しく設定されています。
4) 最後に“quit“と入力後 Enter キーを押すとします。

または、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。
・当該製品を 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。
・当該製品を使用する LAN に信頼できないデバイスが接続されないように、物理的なアクセスを制限してください。

1 https://www.ipa.go.jp/security/vuln/CVSSv3.html
2 https://cwe.mitre.org/data/definitions/489.html

■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

■更新履歴
2023 年 8 月 22 日
「対策方法」に対応済みのシリアル番号を追加しました。