空調管理システムの WEB 機能における権限昇格の脆弱性

公開日 2021 年 7 月 1 日
最終更新日 2021 年 9 月 16 日
三菱電機株式会社

■概要

三菱電機製の空調管理システムの WEB 機能において、認証アルゴリズムの不適切な実装（CWE-303）による権限昇格の脆弱性が存在することが判明しました。これらの脆弱性を攻撃者に悪用された場合、管理者に成りすまされ、当該空調管理システムの設定情報の漏えい、情報の改ざん（空調機器の運転操作や設定値の変更）の影響を受ける恐れがあります。（CVE-2021-20593）

三菱電機製の空調管理システムにおいては、後述の「■脆弱性の説明」にて記載のシステム構成例 1、2 のように、ビル内ネットワークでご使用、もしくは、VPN ルータなどでセキュリティを確保された構成でのご使用を前提としております。ご使用中のシステムが、当社の推奨する適切な構成となっていることをご確認いただけますよう、お願いいたします。

■CVSS スコア

CVE-2021-20593 CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:H/A:N 基本値:7.1

■該当製品の確認方法

＜製品とバージョン＞

【空調管理システム / 集中コントローラー】

型番	バージョン
G-50	Ver.2.50 から 3.35 まで
G-50-W	Ver.2.50 から 3.35 まで
GB-50	Ver.2.50 から 3.35 まで
G-150AD	Ver.3.20 以前のバージョン
GB-50AD	Ver.3.20 以前のバージョン
AE-200J	Ver.7.93 以前のバージョン
AE-50J	Ver.7.93 以前のバージョン
EW-50J	Ver.7.93 以前のバージョン

【空調管理システム / 拡張コントローラー】

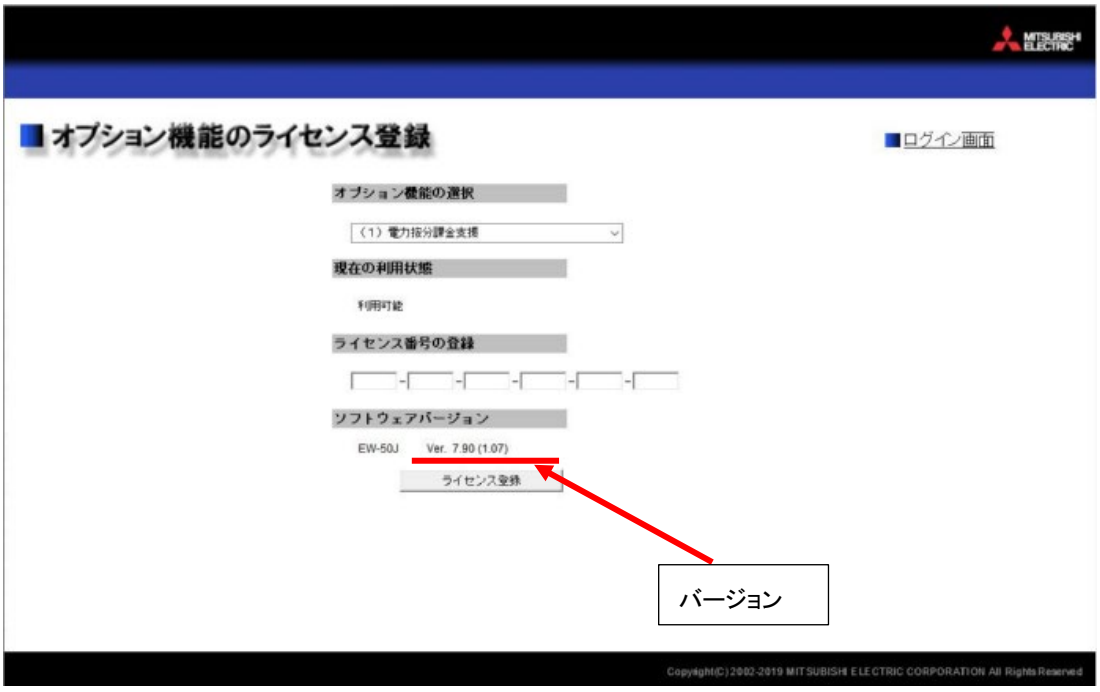
型番	バージョン
PAC-YG50EC	Ver.2.20 以前のバージョン

＜バージョン確認方法＞

各機種で WEB 画面から確認する方法は以下の通りです。

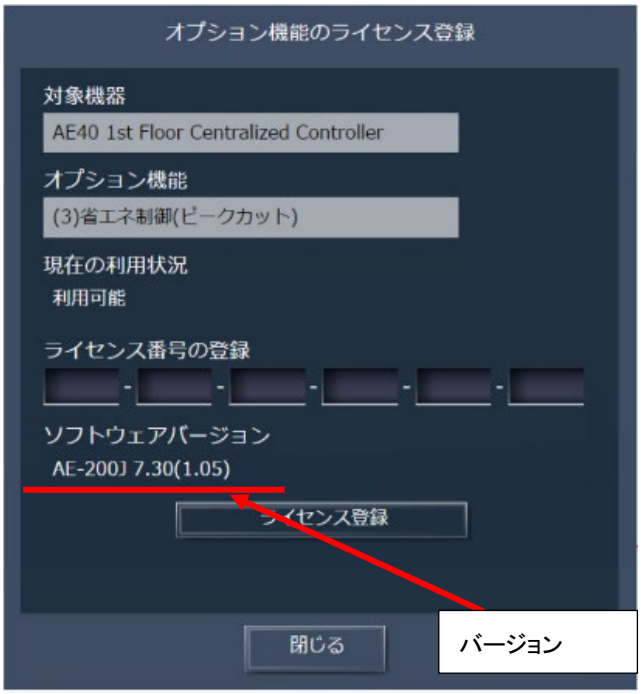
・G-50、G-50-W、GB-50、G-150AD、GB-50AD、PAC-YG50EC の場合

WEB 画面のログイン画面にて「オプション機能のライセンス登録」を選択すると、バージョンを確認できます。



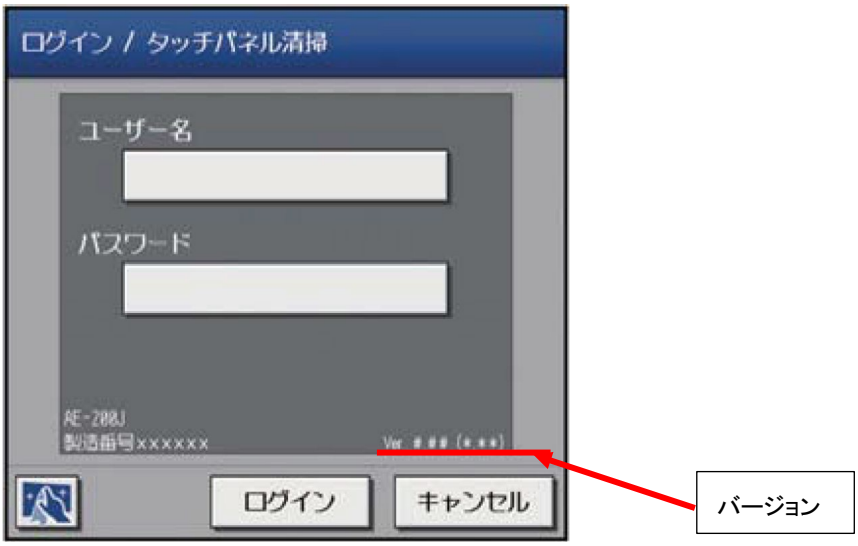
・AE-200J、AE-50J、EW-50J の場合

WEB 画面にて、管理者アカウントでログイン後、ホーム画面の設定タブよりライセンス登録の画面を選択すると、バージョンを確認できます。



・G-150AD、AE-200J、AE-50J の本体画面からのバージョン確認方法

通常画面の右上の設定変更  をタッチしてログイン画面を表示しますと、バージョンを確認できます。



■脆弱性の説明

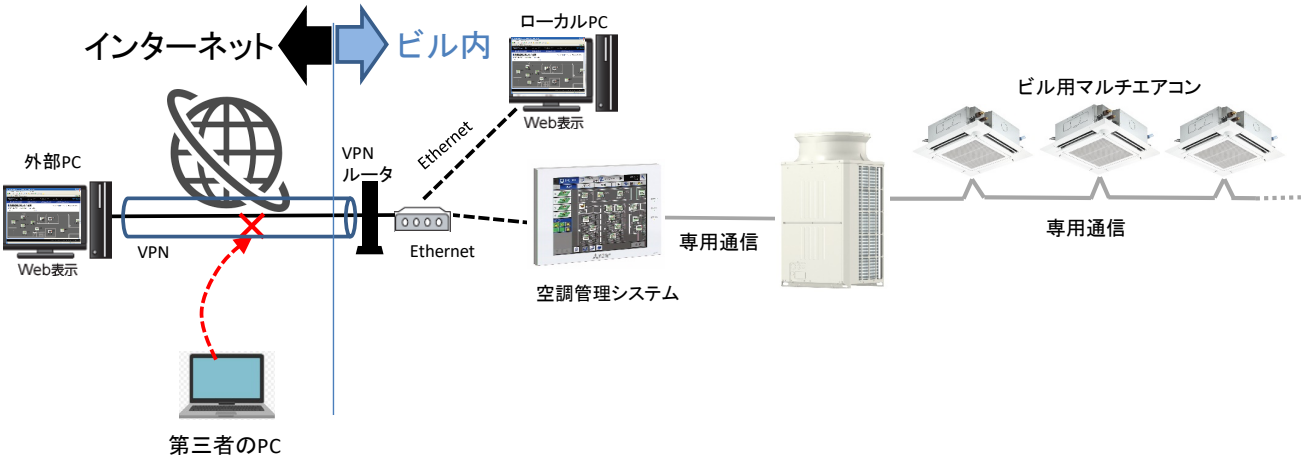
三菱電機製の空調管理システムの WEB 機能には、認証アルゴリズムの不適切な実装（CWE-303）による権限昇格の脆弱性が存在します。

システム構成例 1 や 2 の場合、外部の第三者がインターネットから悪用を試みても、本脆弱性への攻撃は成功しません。

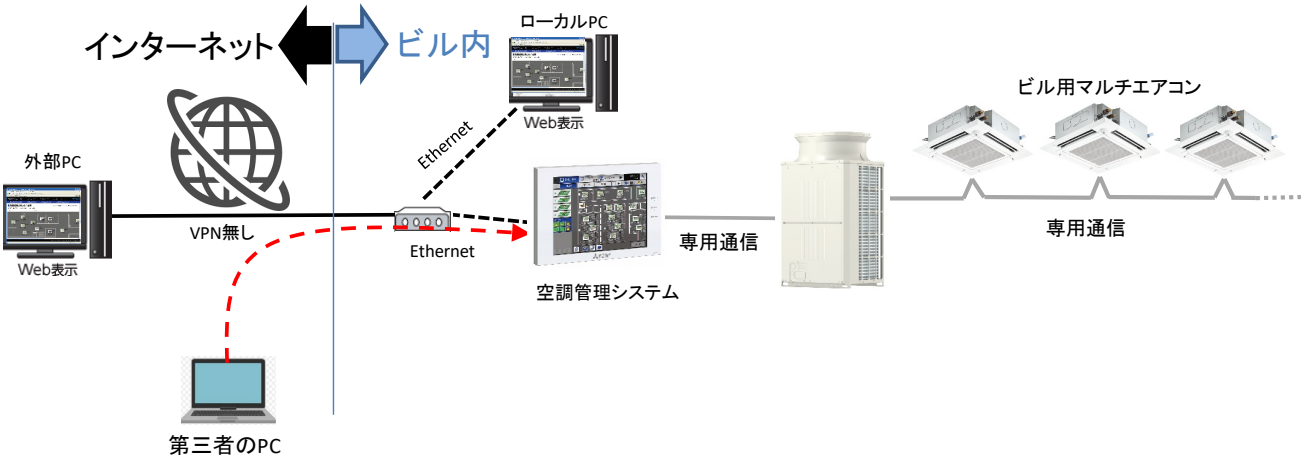
システム構成例 3 の場合、外部の第三者がインターネットから悪用を試みると本脆弱性への攻撃が成功する可能性がございますので、VPN ルータ等、当社が推奨する適切な環境でご使用ください。

システム構成例 1　空調管理システムをビル内のネットワークで使用している構成

システム構成例 2　空調管理システムが VPN ルータを介してビル外の PC からアクセス可能な構成



システム構成例 3　空調管理システムが VPN 無しでビル外の PC からアクセス可能な構成（不適切な構成）



■脆弱性がもたらす脅威

本脆弱性を攻撃者に悪用された場合、権限昇格により管理者に成りすまされ、当該空調管理システムの設定情報の漏えいや情報の改ざん（空調機器の運転操作や設定値の変更）の影響を受ける恐れがあります。

■対策方法

各製品の対策済のバージョンは以下の通りです。

＜製品とバージョン＞

【空調管理システム / 集中コントローラー】

型番	バージョン
G-50	Ver.3.36 以降
G-50-W	Ver.3.36 以降
GB-50	Ver.3.36 以降
G-150AD	Ver.3.21 以降
GB-50AD	Ver.3.21 以降
AE-200J	Ver.7.95 以降
AE-50J	Ver.7.95 以降
EW-50J	Ver.7.95 以降

【空調管理システム / 拡張コントローラー】

型番	バージョン
PAC-YG50EC	Ver.2.21 以降

＜アップデート方法＞

ご購入いただいた販売代理店にお問合せください。ご不明点がございましたら、下記の相談窓口にお問い合わせください。

■軽減策

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、当社が推奨する適切な環境でご使用ください。また、以下に示す軽減策を講じることを推奨します。

・該当製品へのアクセスを、信頼できるネットワークやホストからのアクセスに制限してください。
・ホストにパソコンを用いる場合、パソコンにはウイルス対策ソフトを搭載してください。
・工場出荷時のユーザー名とパスワードを変更してください。

■謝辞

この問題をご報告いただいた Trend Micro の Zero Day Initiative と協力する TXOne IoT/ICS Security Research Labs の Chizuru Toyama 様に感謝いたします。

■お客様からのお問い合わせ先

三菱電機冷熱相談センター TEL 0037-80-2224（携帯電話・PHS の場合 TEL 073-427-2224）

■更新履歴

2021 年 9 月 16 日
「■概要」に情報を追加しました。
「■脆弱性の説明」に影響が生じうるシステム構成例の情報を追加しました。
「■軽減策」の内容を見直しました。