

CB型空調システム制御ボックスにおける情報漏えい、改ざんおよびサービス拒否(DoS)の脆弱性

公開日 2022 年 6 月 7 日
三菱電機エンジニアリング株式会社

■概要

当社CB型空調システム制御ボックスに搭載している三菱電機株式会社製空調管理システムの暗号化通信において、複数の情報漏えい、改ざんおよびサービス拒否(DoS)の脆弱性が存在することが判明しました。これら脆弱性を悪用された場合、攻撃者が暗号化された通信伝文を盗聴することにより、三菱電機株式会社製空調管理システムの一部の情報が漏えいする可能性があります(CVE-2022-24296, CVE-2016-2183, CVE-2013-2566, CVE-2015-2808)。また、攻撃者は、中間者攻撃により、暗号化された通信伝文に不正なメッセージを挿入したり、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-2009-3555)。

三菱電機株式会社製空調管理システムにおいては、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、三菱電機株式会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-2022-24296 CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N 基本値: 3.1
CVE-2016-2183 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N 基本値: 7.5
CVE-2013-2566 CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N 基本値 5.9
CVE-2015-2808 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N 基本値 5.9
CVE-2009-3555 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:H 基本値 7.4

■該当製品の確認方法

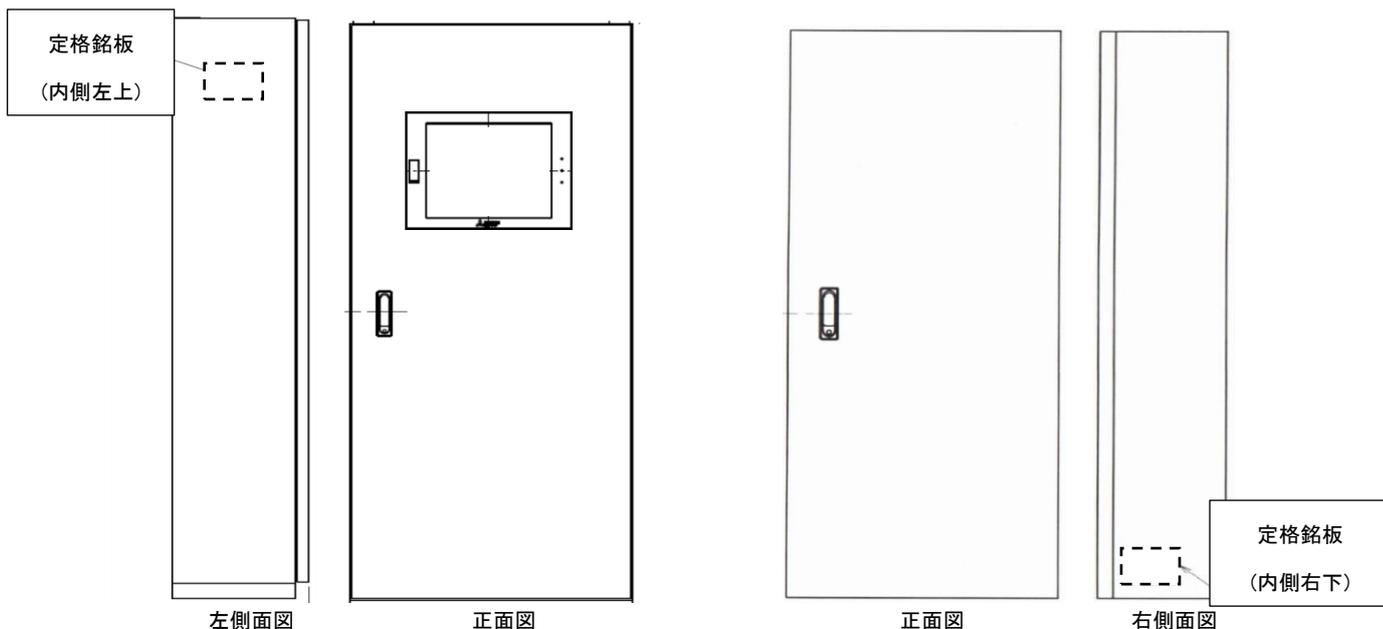
影響を受ける製品は以下の通りです。形名欄の「*」は数字になります。(例:CB-143W1)

<当社製品と三菱電機株式会社製空調管理システムとバージョン>

表の見方...○:該当、×:非該当

当社制御ボックス		対象となる三菱電機製空調管理システム						
形名	影響を受ける製品の範囲	型番	バージョン	CVE-2022-24296	CVE-2016-2183	CVE-2013-2566	CVE-2015-2808	CVE-2009-3555
CB-A***	全ての製品	G-150AD	Ver.3.21 以前	○	○	○	○	○
CB-D***	全ての製品	GB-50AD	Ver.3.21 以前	○	○	○	○	○
CB-E***	全ての製品	GB-50AD	Ver.3.21 以前	○	○	○	○	○
CB-J***	全ての製品	AE-200J	Ver.7.97 以前	○	○	×	×	×
		AE-50J	Ver.7.97 以前	○	○	×	×	×
CB-W***	全ての製品	AE-200J	Ver.7.97 以前	○	○	×	×	×
		EW-50J	Ver.7.97 以前	○	○	×	×	×
CB-***W*	製造年月 2022 年 5 月 以前	AE-200J	Ver.7.97 以前	○	○	×	×	×
		AE-50J	Ver.7.97 以前	○	○	×	×	×
		EW-50J	Ver.7.97 以前	○	○	×	×	×

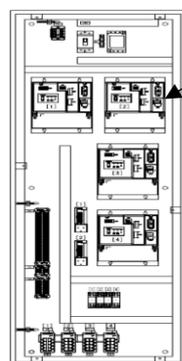
[形名確認方法] 制御ボックス内側(左上もしくは右下)の定格銘板をご確認ください。(下図は代表形状です)



[銘板例]

MEE	CB型空調システム制御ボックス
形名	CB-W***
電源	
消費電力	
質量	
製造番号	
製造年月	
三菱電機エンジニアリング株式会社	

[内部配置図]



CB型空調システム制御ボックス内に三菱電機製空調システムを搭載しております。

脆弱性が確認された三菱電機製空調管理システムとバージョンの確認は以下を参照してください。
<https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2022-005.pdf>

三菱電機製空調管理システムのバージョンをご確認いただいた結果、対象ではなかった場合は下記「**■対策方法**」は不要になります。

■脆弱性の説明

当社CB型空調システム制御ボックスに搭載している三菱電機製空調管理システムの暗号化通信において、以下の複数の情報漏えいの脆弱性(CVE-2022-24296、CVE-2016-2183、CVE-2013-2566、CVE-2015-2808)および情報の改ざん、サービス拒否(DoS)の脆弱性(CVE-2009-3555)が存在します。

- ・CVE-2022-24296: 不完全、または危険な暗号アルゴリズムの使用(CWE-327)
- ・CVE-2016-2183: 情報漏えい(CWE-200)
- ・CVE-2013-2566: 不完全、または危険な暗号アルゴリズムの使用(CWE-327)
- ・CVE-2015-2808: 不完全、または危険な暗号アルゴリズムの使用(CWE-327)
- ・CVE-2009-3555: 中間者攻撃問題(CWE-300)

詳細は、以下を参照してください。

<https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2022-005.pdf>

■脆弱性がもたらす脅威

これら脆弱性を攻撃者に悪用された場合、当該機器との通信情報の一部が漏えいしたり、改ざんされたり、対象が DoS 状態に陥る可能性があります。

■対策方法

当社CB型空調システム制御ボックスに搭載している三菱電機製空調管理システムの対策済のバージョンとアップデート方法は以下を参照してください。

<https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2022-005.pdf>

■回避策

これらの脆弱性が悪用されることによるリスクを回避するため、三菱電機が推奨する適切な環境でご使用ください。また、三菱電機エンジニアリングは以下に示す回避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。
- ・アクセス元のパソコンの OS や WEB ブラウザを最新のバージョンに更新し、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

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)