

# 省エネデータ収集サーバ(EcoServerⅢ)および 検針コントローラの Web 機能における複数の脆弱性

公開日 2022 年 2 月 15 日  
三菱電機株式会社

## ■概要

省エネデータ収集サーバ(EcoServerⅢ)および検針コントローラに搭載している複数の OSS(オープンソースソフトウェア)に、複数の脆弱性が存在することが判明しました。これらの脆弱性を悪意のある攻撃者に悪用された場合、当該製品の情報の漏えいや改ざんが起きたり、当該製品がサービス拒否(DoS)状態に陥る可能性があります。(CVE-2016-10735、CVE-2017-18214、CVE-2018-14040、CVE-2018-14042、CVE-2018-20676、CVE-2019-8331、CVE-2020-7746、CVE-2020-11022、CVE-2020-11023)

これらの脆弱性の影響を受ける省エネデータ収集サーバ(EcoServerⅢ)および検針コントローラのバージョンを以下に示しますので、該当製品については対策方法あるいは軽減策・回避策に記載の内容を実施してください。

## ■CVSS スコア

・CVE-2016-10735	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	基本値:6.1
・CVE-2017-18214	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	基本値:7.5
・CVE-2018-14040	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	基本値:6.1
・CVE-2018-14042	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	基本値:6.1
・CVE-2018-20676	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	基本値:6.1
・CVE-2019-8331	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	基本値:6.1
・CVE-2020-7746	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	基本値:7.5
・CVE-2020-11022	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	基本値:6.1
・CVE-2020-11023	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	基本値:6.1

## ■該当製品の確認方法

影響を受ける製品の形名、バージョンは以下のとおりです。

製品	形名	バージョン
省エネデータ収集サーバ (EcoServerⅢ)	MES3-255B	3.0.0 ~ 3.3.0
	MES3-255B-DM	
	MES3-255C	
	MES3-255C-DM	
検針コントローラ	B-AM500LN	2.0.0 ~ 2.2.0
	B-AM1000LN	
	B-AM100SN	
	B-AM300SN	
	B-AM500SN	

バージョンの確認方法は、以下の通りです。

### 【省エネデータ収集サーバ(EcoServerⅢ)】

取扱説明書:運用編の【第 3 章 3.3 バージョンの確認方法】をご参照ください。

※三菱電機 FA サイト(<https://www.mitsubishielectric.co.jp/fa/>)内ダウンロードページより最新の取扱説明書入手ください。

### 【検針コントローラ】

取扱説明書:運用編の【第 3 章 5.1 バージョンの確認方法】をご参照ください。

※三菱電機 FA サイト(<https://www.mitsubishielectric.co.jp/fa/>)内ダウンロードページより最新の取扱説明書入手ください。

## ■脆弱性の説明

省エネデータ収集サーバ(EcoServerⅢ)および検針コントローラには、以下に示すクロスサイトスクリプティング(CWE-79)の脆弱性により、情報漏えいまたは情報改ざんが起きる可能性があります。

- ・CVE-2016-10735: クロスサイトスクリプティング(CWE-79)
- ・CVE-2018-14040: クロスサイトスクリプティング(CWE-79)
- ・CVE-2018-14042: クロスサイトスクリプティング(CWE-79)
- ・CVE-2018-20676: クロスサイトスクリプティング(CWE-79)
- ・CVE-2019-8331 : クロスサイトスクリプティング(CWE-79)
- ・CVE-2020-11022: クロスサイトスクリプティング(CWE-79)
- ・CVE-2020-11023: クロスサイトスクリプティング(CWE-79)

また、省エネデータ収集サーバ(EcoServerⅢ)および検針コントローラには、以下に示すリソースの枯渇(CWE-400)および動的に決定されたオブジェクト属性の不適切に制御された変更(CWE-915)の脆弱性により、サービス拒否(DoS)状態に陥る可能性があります。

- ・CVE-2017-18214: リソースの枯渇(CWE-400)
- ・CVE-2020-7746 : 動的に決定されたオブジェクト属性の不適切に制御された変更(CWE-915)

## ■脆弱性がもたらす脅威

これらの脆弱性を悪意のある攻撃者に悪用された場合、当該製品の情報の漏えいや改ざんが起きたり、当該製品がサービス拒否(DoS)状態に陥る可能性があります。

## ■対策方法

対策済みのバージョンは以下のとおりです。

製品	形名	バージョン
省エネデータ収集サーバ (EcoServerⅢ)	MES3-255B	3.3.1 以降
	MES3-255B-DM	
	MES3-255C	
	MES3-255C-DM	
検針コントローラ	B-AM500LN	2.2.1 以降
	B-AM1000LN	
	B-AM100SN	
	B-AM300SN	
	B-AM500SN	

### 【省エネデータ収集サーバ(EcoServerⅢ)】

該当バージョンをご使用のお客様は、以下のマニュアルをご参照の上、バージョンアップを実施ください。

- ・省エネデータ収集サーバ EcoServerⅢ 本体プログラム、設定ソフトウェア バージョンアップ手順書
- ※三菱電機 FA サイト(<https://www.mitsubishielectric.co.jp/fa/>)内ダウンロードページより入手ください。

### 【検針コントローラ: B-AM500LN/ B-AM1000LN】

該当バージョンをご使用のお客様は、リモートプログラム書き込みソフトウェアに同梱している以下のマニュアルをご参照の上、バージョンアップを実施ください。

- ・検針コントローラ(モデル L)バージョンアップ操作手順書
- ※三菱電機 FA サイト(<https://www.mitsubishielectric.co.jp/fa/>)内ダウンロードページより入手ください。

### 【検針コントローラ: B-AM100SN/ B-AM300SN / B-AM500SN】

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する。
- ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。

## ■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>