HITACHI
Inspire the Next

# IoT 対応産業用コントローラ HX-CPU モジュールにおける ディレクトリトラバーサル問題について(CVE-2018-25048)

**セキュリティ情報 ID:hitachi-sec-2022-002**

株式会社 日立産機システム

## ■ 概要

HX-CPU モジュールに搭載している CODESYS ランタイムには、ディレクトリトラバーサル(ファイルの閲覧・参照)に起因し、システム設定ファイルの変更を許してしまう脆弱性(CVE-2018-25048)が存在します。

## ■ 対象製品

影響を受ける製品の型式およびソフトウェアバージョンは以下の通りです。

| 品名 | 型式 | ソフトウェアバージョン |
|---|---|---|
| HX シリーズ CPU モジュール | HX-CP1S08/-0 | 3.5.16.25 および それ以前のバージョン |
| | HX-CP1H16/-0 | |
| | HX-CP1S08M/-0 | |
| | HX-CP1H16M/-0 | |
| | HXC-CP1H16/-0 | |

ソフトウェアバージョンの確認方法はマニュアルを参照してください。マニュアルは、弊社の Web サイトからダウンロードして入手することができます。

## ■ 想定される影響

認証されていない遠隔の第三者によりシステム設定ファイルの変更を許してしまう可能性があります。

## ■ 対策方法

・ 以下のソフトウェアバージョンで対策済みです。

| 品名 | 型式 | ソフトウェアバージョン |
|---|---|---|
| HX シリーズ CPU モジュール | HX-CP1S08/-0 | 3.5.16.26 |
| | HX-CP1H16/-0 | |
| | HX-CP1S08M/-0 | |
| | HX-CP1H16M/-0 | |
| | HXC-CP1H16/-0 | |

ソフトウェアバージョンアップサービス(有償)については、お問い合わせください。

・ システム設定ファイル更新により対策できるものがあります。詳しくは弊社までお問い合わせください。

## ■ 軽減策、回避策

本製品につきましては、マニュアルに記載されている安全上の注意に従ってご使用いただくことを推奨しています。

- 守るべきプログラムやデータに対する認証機能の活用と定期的な見直し
- ネットワークを構成する機器のセキュリティ機能の活用
- 接続相手を特定する機能の活用による不特定の相手との接続の防止
- 機器の設置場所の施錠や操作者を限定するなどの運用管理での対策

脆弱性のリスクに対する緩和策として以下を推奨します。

- 保護された環境でのみコントローラとデバイスを使用して、ネットワークへの露出を最小限に抑え、外部からアクセスできないようにします。
- ファイアウォールを使用して、制御システム ネットワークを保護し、他のネットワークから分離します。
- リモート アクセスが必要な場合は、VPN (Virtual Private Networks) トンネルを使用します。
- ユーザー管理とパスワード機能を有効にして適用します。
- 開発システムと制御システムの両方へのアクセスを、物理的な手段、オペレーティングシステムの機能などによって制限します。
- 最新のウイルス検出ソリューションを使用して、開発システムと制御システムの両方を保護します。

■ 関連情報

CVE-2018-25048

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-25048>

Advisory 2018-04: Security update for CODESYS V2 and V3 runtime systems

<https://customers.codesys.com/fileadmin/data/customers/security/2018/Advisory2018-04_CDS-59017.pdf>

■ お問い合わせ先

以下の製品サポート窓口にお問い合わせください。

<https://www.hitachi-ies.co.jp/products/hx/index.html>

■ 商標

CODESYS は、CODESYS GmbH の登録商標です。

■ 管理番号、更新履歴

| 管理番号 | 日付 | レビジョン | |
|---|---|---|---|
| HIES-SEC-2023-01 | 2023 年 2 月 6 日 | Rev.1 | 新規作成および公開 |