

# Yokogawa Security Advisory Report

YSAR-22-0007

公開日 2022/6/21  
最終更新日 2022/6/29

## YSAR-22-0007: STARDOM に複数の脆弱性

### 概要:

STARDOM に複数の脆弱性が存在することが判明しました。以下に、影響を受ける製品をご案内いたします。

本レポートの内容をご確認の上、影響を受ける製品を含むシステム全体のセキュリティ対策などを総合的にご判断いただき、必要に応じて対策の適用をご検討ください。

### 影響を受ける製品:

下記脆弱性詳細 1 の影響を受ける製品

- STARDOM FCN/FCJ R1.01 - R4.31

下記脆弱性詳細 2 の影響を受ける製品

- STARDOM FCN/FCJ R4.10 - R4.31

### 脆弱性詳細 1:

攻撃者が FCN/FCJ コントローラーとの通信を傍受し認証情報を窃取した場合、コントローラーの設定変更や改ざんされたファームウェアの更新が行われる可能性があります。

- ・重要な情報の平文での送信 ([CWE-319](#))

[CVE-2022-29519](#)

CVSS v3 基本値: 4.8

[CVSS:3.0/AV:A/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N](#)

### 脆弱性詳細 2:

攻撃者がハードコードされた認証情報を窃取した場合、コントローラーの設定変更や改ざんされたファームウェアの更新が行われる可能性があります。\*

\* 窃取された認証情報でコントローラーへログインできるのは、FCN/FCJ CPU モジュールが二重化構成された環境のみです。

(CPU シングル構成の環境ではログイン不可)

- ・ハードコードされた認証情報の使用 ([CWE-798](#))

[CVE-2022-30997](#)

CVSS v3 基本値: 6.3

[CVSS:3.0/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H](#)

### 対策方法:

脆弱性詳細 1, 2 の対策方法

以下の緩和策を適用してください

- FCN/FCJ のパケットフィルタ機能\*1を使用し、適切な送信元からの通信のみを許可するように設定する
- 攻撃者に通信を傍受されないよう適切なネットワーク制御を行う

今回確認された脆弱性に限らず、システム全体において適切なセキュリティ対策\*2を講じていただくことを横河は推奨しています。

\*1 パケットフィルタ機能を使用するには、FCN/FCJ 基本ソフトウェアを R4.20 以降にレビジョンアップしてください。

レビジョンアップ作業を横河電機にご依頼いただいた場合、同作業のコストはお客様負担となります。

\*2 対策例としては、パッチ適用、アンチウィルス、ホワイトリスティング、ハードニング、バックアップ、ファイアウォール、ネットワークセグメンテーション、などがあります。

#### サポート:

● 本レポートの内容に関するご質問等については、下記サイトからお問い合わせください。

<https://contact.yokogawa.com/cs/gw?c-id=000523>

#### 謝辞:

本脆弱性は以下の方々により発見・通知されました。

● Jos Wetzels, Forescout

#### 参考:

1. CVSS（共通脆弱性評価システム）について

<https://www.ipa.go.jp/security/vuln/CVSSv3.html>

共通脆弱性評価システム CVSS（Common Vulnerability Scoring System）は、情報システムの脆弱性に対するベンダーに依存しない汎用的な評価手法です。脆弱性の深刻度を同一の基準の下で定量的に比較できるようになります。

本レポートに記載されている CVSS の各値は現状のまま提供するものであり、いかなる保証も伴いません。

本レポートに記載されている脆弱性が実際にどれだけの深刻度があるかについては、影響を受ける製品を含むシステム全体のセキュリティ対策などを総合的に判断した上で、お客様自身で評価していただく必要があります。

#### 更新履歴:

2022/6/21: 初版

2022/6/29: 対策方法を更新

※本レポートの内容については、将来予告なしに変更することがあります。