Yokogawa Security Advisory Report

YSAR-16-0002

公開日 2016-9-14
最終更新日 2016-9-14

YSAR-16-0002: STARDOM コントローラに任意のコマンドを実行される脆弱性

概要:

STARDOM コントローラおよびロジックデザイナにおいて、接続に認証を要求しないため、第三者に任意のコマンドを実行されてしまう脆弱性が存在することを確認しました。以下に、この脆弱性の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:

下記影響を受ける製品に脆弱性が存在します。
・STARDOM FCN/FCJ （R1.01～R4.01）

脆弱性詳細:

ロジックデザイナは、認証無しに STARDOM コントローラと接続できるため、第三者により IEC アプリケーションの停止、値の書き換え、アプリケーションの変更などが実行できてしまう危険性があります。

CVSS v2 における本脆弱性の基本値は 7.5、現状値は 6.2 です。

攻撃元区分(AV)	ローカル(L)	隣接(A)	ネットワーク(N)
攻撃条件の複雑さ(AC)	高(H)	中(M)	低(L)
攻撃前の認証要否(Au)	複数(M)	単一(S)	不要(N)
機密性への影響(C)	なし(N)	部分的(P)	全面的(C)
完全性への影響(I)	なし(N)	部分的(P)	全面的(C)
可用性への影響(A)	なし(N)	部分的(P)	全面的(C)

攻撃される可能性(E)	未実証(U)	実証可能(POC)	攻撃可能(F)	容易に攻撃可能(H)	未評価(ND)
利用可能な対策レベル(RL)	正式(OF)	暫定(TF)	非公式(W)	なし(U)	未評価(ND)
脆弱性情報の信頼性(RC)	未確認(UC)	未確証(UR)	確認済(C)	未評価(ND)	

対策方法:

最新版の R4.02 にアップデートすることで本脆弱性が修正されます。
アップデート方法等は下記サポートまでお問い合わせください。

なお、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を講じていただくことを推奨しています。

All Rights Reserved. Copyright © 2016, Yokogawa Electric Corporation

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、下記にお問い合わせください。
http://stardom.jp

参考:

1. CVSS(共通脆弱性評価システム)について
   http://www.ipa.go.jp/security/vuln/CVSS.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:

2016-9-14: 初版

※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。

All Rights Reserved. Copyright © 2016, Yokogawa Electric Corporation