FR Configurator2 における XML の脆弱性

公開日 2019 年 7 月 23 日
三菱電機株式会社

■概要

FR Configurator2 のバージョン 1.16S 以前に XML に起因する複数の脆弱性が存在することが判明しました。この脆弱性を悪用された場合、悪意ある第三者の攻撃により、FR Configurator2 が動作しているコンピュータ上のファイルが外部に送信される、もしくは、FR Configurator2 が応答なしになる危険性があります。

この問題の影響を受ける FR Configurator2 のバージョンを以下に示しますので、対策済バージョンにバージョンアップしてください。

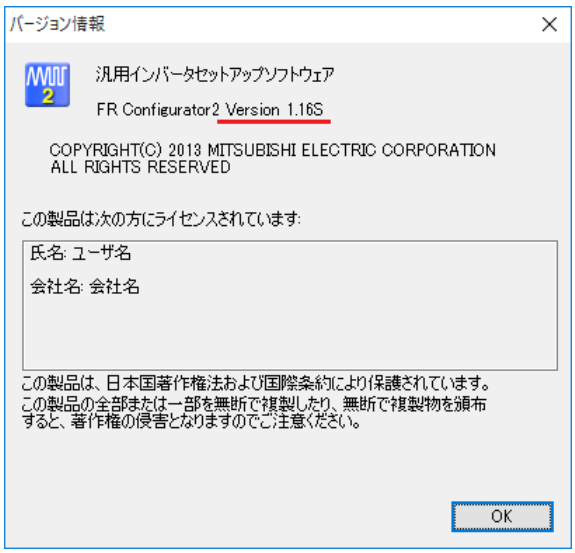
■該当製品の確認方法

影響を受ける製品とバージョンは以下の通りです。

製品名称　　FR Configurator2
製品形名　　SW1DND-FRC2-J もしくは SW1DND-FRC2-E
該当バージョン　1.16S 以前の全てのバージョン

使用しているバージョンの確認方法は以下の通りです。

1, FR Configurator2 を起動し、「ヘルプ」メニューから「バージョン情報」を選択する。
2. 現れたウィンドウの下記の部分が起動している FR Configurator2 のバージョン番号です。



■脆弱性の説明

FR Configurator2 には、XML に起因する次の複数の脆弱性が存在します。

・XML 外部エンティティ参照の不適切な制限(CWE-611) - CVE-2019-10976
・リソースの枯渇 (CWE-400) - CVE-2019-10972

■脆弱性がもたらす脅威

攻撃者により不正に細工された FR Configurator2 のプロジェクトファイルを誤って開くことにより、次のような影響を受ける可能性があります。

・ユーザ権限でアクセス可能な任意のファイルが外部に送信される
・FR Configurator2 が応答なしになる

■対策方法

FR Configurator2 バージョン 1.16S 以前の製品を利用されているお客様は、対策済バージョンをインストールしてください。

修正プログラムのダウンロード

SW1DND-FRC2-J
https://www.mitsubishielectric.co.jp/fa/download/software/detailsearch.do?mode=software&kisyu=/inv&shiryoid=0000000020&lang=1&select=0&softid=1&infostatus=1_2_1&viewradio=0&viewstatus=10_0_0_100_0&viewpos=0_0
SW1DND-FRC2-E
https://www.mitsubishielectric.co.jp/fa/download/software/detailsearch.do?mode=software&kisyu=%2Finv&kisyuid=10&shiryoid=0000000023&lang=1&select=0&softid=1&infostatus=1_2_1&viewradio=0&viewstatus=10_0_0_100_0&viewpos=0_0

■回避策
信頼できない発信元や出処が不明なプロジェクトファイルは開かないように注意してください。

■謝辞
この問題をご報告いただいた、Applied Risk 社に感謝いたします。

■お客様からのお問い合わせ先
お買上店または当社営業所までお問い合わせください。